ISSN 1879-9523
journal of chain-computerisation
information exchange for chain co-operation
Universiteit Utrecht

Founding article

A Chain Perspective on Large-scale Number Systems

J.H.A.M. Grijpink

Journal of Chain-computerisation
Information Exchange for Chain Co-operation

2012 – Volume 3, Art. #2

Received: 2 July 2012
Accepted: 25 August 2012
Published: 17 September 2012

2012 – Volume 3, Art. #2
URN:NBN:NL:UI:10-1-113821
ISSN: 1879-9523
URL: http://jcc.library.uu.nl/
Publisher: Igitur publishing, in co-operation with the Department of Information and Computing Sciences, Utrecht University

Copyright: this work is licensed under a Creative Commons Attribution 3.0 License

A Chain Perspective on Large-scale Number Systems[1]

J. (Jan) H.A.M. Grijpink
Emeritus Professor,
Utrecht University, The Netherlands
j.h.a.m.grijpink@uu.nl

Abstract: As large-scale number systems gain significance in social and economic life (electronic communication, remote electronic authentication), the correct functioning and the integrity of public number systems take on crucial importance. They are needed to uniquely indicate people, objects or phenomena in the ever-increasing digitisation of our information society. Number systems fulfil many functions, often several at the same time. Due to poor system design and management people can in many ways manipulate number systems or number verifications to claim rights or other advantages and to render oneself invisible and untraceable by hiding behind somebody else’s personal number. In practice, a personal number is often used as claim of identity, both online and offline, both honestly and dishonestly. At present, our large-scale number systems are vulnerable to the misuse of personal numbers (identity fraud/theft). Moreover, the usual multi-chain usage of large-scale personal number systems turns out to be very problematic.

Thus, the design and management of number systems are becoming more and more vital to our information society. Unfortunately, the study of large-scale number systems has long been neglected in Public Administration Science as well as in Information Science. To fill this gap this article presents a number system theory based on the theory of Chain-computerisation. It explaines some important insights that have to be taken into account when designing, implementing and managing large-scale number systems.

Keywords: authentication, large-scale personal number system, Chain-computerisation, information strategy, identity management, interoperability, privacy, security

1 Introduction

Decisions about large-scale number systems are of great importance to our emerging information society, because number systems are needed to register and to exchange information about people, objects or phenomena. Unfortunately, the study of large-scale number systems has long been neglected in Public Administration Science as well as in Information Science.

Politicians, public administrators and information professionals are nevertheless confronted with difficult strategic choices regarding design, implementation and management of number systems. Choices must be made between:

a. The exclusive use of a general (=all-purpose) number and the non-exclusive use of a set of several independent (chain) numbers;
b. Adopting an existing personal number for a new purpose and introducing a new tailor-made personal number (Grijpink, 2002b);

[1] I thank Prof.dr. S.D. Swierstra and Dr. M.G.A. Plomp for their valuable remarks.

c. A personalised number, a pseudonym and an entirely anonymous number (Grijpink & Prins, 2003);
d. An interoperable number system that can accommodate numbers from other similar number systems and a non-interoperable number system (Hayat, Posch & Rössler, 2005);
e. A public and a private number system.

Shortcomings in design and implementation of large-scale systems are difficult or impossible to remedy afterwards.

This article presents a theoretical framework for the design, implementation and management of number systems based on the theory of Chain-computerisation (Grijpink, 1997, 2000a, 2000b). It builds on prior publications on number systems, identity fraud and biometrics (Grijpink, 2002b, 2004, 2006, 2008). It explaines some important insights that have to be taken into account.

We especially focus on personal number systems but insights that apply to personal numbers are often applicable to other numbers.

In this section 1 some core concepts are introduced: number system, number system application, identity, identity management, chain perspective and number strategy. The following sections 2-4 elaborate on some important characteristics, legal aspects of number systems and key issues regarding number strategies. Section 5 presents a summarising checklist for a more robust design, implementation and management of large-scale number systems.

1.1 Number system and number system application

A number system is a system based on a series of numbers used to uniquely indicate an individual instance within a defined or definable group of persons, objects or phenomena. This number can also be used as a key to retrieve data from databases that are related to this instance.

Numbers can be numerical (purely digits) or alphanumerical (digits and letters).

The term 'system' is taken to mean that the number is assigned and later withdrawn according to certain rules, and that the use of the number is subjected to certain rules, as well. Table 1 shows some examples of number systems.

Table 1. Examples of number systems

1	serial number at the butcher's
2	postal code + house number
3	car registration number
4	document number (e.g. passport number)
5	road number
5	telephone number
6	Internet address (IP address)
7	client number
8	bank account number
9	citizen service number (Burgerservicenummer, BSN)

In this article the concept of 'number system application' is used to indicate that any number system can be considered being implemented within a larger context characterised by dimensions such as geographic area, domain, purpose and degree of voluntary use.

1.2 Identity management and number systems

The increasing use of numbers in electronic data processing is a phenomenon that is inherent in the advancing computerisation of our society. In practice, a personal number is often used as claim of identity, both online and offline, both honestly and dishonestly. Rightly or wrongly, numbers enable claiming rights or other advantages and facilitate rendering oneself invisible and untraceable by hiding behind somebody else's personal number.

This dual use of numbers is also revealing the vulnerability of number systems if not properly designed, implemented and managed. It turns out that there are many ways to frustrate number verifications, and identity fraud using personal numbers is rising sharply. At present, the attention paid to the misuse of personal numbers mainly focuses on breaches of privacy, but that should be extended more and more to security breaches. A compromised personal number can result in the victim having to spend years defending himself against a wrongful suspicion or conviction, followed by a bitter struggle to restore his reputation or recover his loss. Often in vain, for the victim is initially taken as the perpetrator (after all, the victim's personal number has been used!), and is often unable to prove his innocence. This underlines that privacy and security are becoming increasingly intertwined. Therefore, in our privacy debates, we should direct our attention more and more towards regulating the use of identities, preventing identity fraud and privacy enhancing use of large-scale number systems, three essential elements of identity management.

1.3 The chain perspective on number systems

Number systems can be used by collaborating autonomous organisations and independent professionals. This interorganisational collaboration is not easy, because there exists no all-encompassing authority in a chain, as a result of which chain-wide decision-making processes are unclear and irrational (Grijpink, 1997, pp. 131-144; 2002a, pp. 19-31; 2010b, pp. 27-36). Because of this absence of hierarchy, the theory of Chain-computerisation conceives a chain as a temporary pattern of interorganisational co-operation triggered and enforced by a dominant chain problem. This is a disrupting problem for every chain partner while no one can solve this problem alone. It calls for a chain-specific structural partnership to prevent a chain from being disrupted by systematic failure to deliver its social product (health, security, prosperity).

This dominant chain problem differs between chains. In the stockbreeding chain, for instance, the chain partners have to prevent unhealthy meat getting into our food; any chain partner can frustate this chain's challenge unless preventive mechanisms are robust enough to detect unhealthy meat. Therefore, undetected health risk is the dominant chain problem here. Another example is from the criminal law enforcement chain. Criminals try to commit crimes undetected or, if caught, try to evade punishment. Using somebody else's identity can do this. The Dutch champions in this respect have succeeded in using more than fifty identities (Grijpink, 2004; 2006). By accepting a wrong identity any policeman can disrupt the criminal law enforcement chain unless this chain can detect aliases. If not, criminal cases cannot be solved, victims are treated as suspects and criminal law enforcement degrades to a senseless social activity. So, identity fraud is the dominant chain problem in the criminal law enforcement chain.

The theoretical framework for the design, implementation and management of number systems presented in the following sections is predominantly based on this chain perpective. Only when a number system is absolutely indispensable to solving the dominant chain problem, there will be sufficient support in this chain for a common management of the number system in accordance with the requirements set by that specific dominant chain problem. The more direct the relation of a number system with its dominant chain problem, the more its management can benefit from this support and from chain-specific self-cleaning and self-resolving mechanisms.

1.4 Number strategies

With 'number strategy' we mean the dynamic complex interaction pattern of general and chain number systems resulting from government measures and behaviour of number users and number system managers. The concept 'number strategy' can be illustrated with the example of the Dutch number strategy.

> Example **The Dutch number strategy**
> For decennia Dutch residents have been registered using a confidential administration (A-) number and a confidential fiscal (FI-) number. The A-number has been kept confidential, but since 1985 the FI-number has been regarded as a public number which was also introduced in the social security sector in 1988: the Dutch SOFI-number came into being. In 2001 the Dutch legislator decided that this SOFI-number could also serve as the official education number. In 2007 the SOFI-number was renamed Citizen Service Number (Burgerservicenummer, BSN) by law and assigned the role of general personal number to be compulsorily used by all government agencies. In June 2008, this BSN was also introduced in the predominantly private health care sector to be compulsorily used for storing and exchanging medical data. Step-by-step the Dutch number strategy is moving towards a mandatory general personal number system, which - because of compulsory use – will gradually replace existing chain number systems and prevent new ones from being introduced.
> Then the behaviour of number managers and number users must be taken into account. Since the introduction of the SOFI-number in the social security domain identity fraud has been increasing sharply. The SOFI-number is often used as claim of identity enabling access or benefiting from rights or other advantages, with or without malicious intent. Nowadays, many people have been wrongly issued more than one BSN; others make use of someone else's BSN, with or without the consent of the rightful holder. This way, the BSN number system is gradually corrupting many important public databases, e.g. criminal and medical records.

This example of the Dutch SOFI/BSN-number shows what can happen with any number system unless its design, implementation and management guarantee that the numbers are being sufficiently guarded and protected against misuse after being issued. If this is in fact possible depends on the type of national number strategy in place. Large-scale number systems, especially mandatory general public personal number systems, are difficult to manage without overlapping personal data in other independent sources. Consistency checks with these data can prevent errors from spreading undetected and limit the damage caused by deliberate manipulation because very few people are able to manipulate data in various independent systems in the same way at the same time. In the case of a mandatory general public personal number system these independent chain number systems with overlapping personal data are gradually replaced by the general number system itself and no longer available for consistency checks. So, if a mandatory general public personal number system is at the core of a national number strategy, preventing or detecting errors and fraud in this number system and related databases is very problematic.

2 Characteristics of a number

Five characteristics of a number are discussed in this section: (1) the function of a number, (2) the scope of application, (3) the unicity of a number, (4) the number format and (5) the number semantics. Combinations of these characteristics result in specific applications with pros and cons. These offer a great diversity of possible solutions to those designing, implementing or managing a number system.

2.1 Function of a number

Numbers fulfil many functions - often several at the same time - based on the ability to uniquely indicate a single instance in a series. A case in point is when one wishes to lay down a detail in a register or follow a certain sequential order, as a butcher would, for instance. By using a number it is possible to trace a detail and also establish that two details are related. When comparing details of the same person or object from various sources, linking with numbers is often more accurate than linking with words only (e.g. name and address details) or images (e.g. photograph, signature, logo). Take into account that foreign names can be written in different ways and that certain names can be very common. Moreover, consider that some information systems do not allow correct and unambiguous registration due to a limited character set e.g. without diacritical marks.

Using numbers one can detect that - against the rules of the number system - somebody is using several unique personal numbers at the same time or – conversely - that a supposedly unique personal number is being used by several people at the same time.

If a number contains a property of a person or object, this information can easily be passed on to somebody else by using the number (e.g. year of birth, sex, expiry or place of issue). Random numbers, conversely, can protect against this function of implicit information transfer.

2.2 Scope of application

Numbers have a certain scope of application. We focus on two dimensions of an application: content and geographical range. The butcher’s serial number is used for serving customers (the content aspect) locally in the shop (the geographical aspect). A car registration number relates to cars and road traffic in all its aspects (content) and can, depending on the country of registration, be used by everybody, both nationally and internationally (the geographical range).

Elaborating on the content dimension, there are both sectoral and chain numbers. As we will see in subsection 4.2, with ‘chain’ we have a more specific scope of application in mind than with ‘sector’. In the theoretical framework of Chain-computerisation, a sector, e.g. health care, consists of a number of separate chains depending on the various different dominant chain problems, for instance cancer treatment, drug addicts’ care or diabetes care. Numbers can also be applied in more than one sector or chain (content). We call these numbers multi-sectoral or multi-chain numbers. In the content dimension, finally, there are general (= all-purpose) numbers.

In the geographical dimension, national and international numbers stand out between local, regional and global numbers.

Within the entire geographical area of application the use of a number does not have to be the same. In the one region a chain can use its own chain number, for example, while the same chain in another region uses a national number. In the same way, one region (geographic dimension) can use a multi-chain number (content dimension) while another region (geographic dimension) has a dedicated chain number of its own (content dimension).

Running ahead of our later analysis in subsection 4.3, it is interesting to mention here the gradual change in the scope of application of the Dutch SOFI-number/BSN as explained in subsection 1.4. Within twenty years, the SOFI-number developed from a confidential tax number towards a compulsory general public number.

2.3 Unicity

A number’s unicity has at least two dimensions: place and time. Keep in mind that unicity is a relative characteristic, depending on other characteristics such as function, scope or semantics.

A house number is unique within the geographical limitation of the street. It is more related to a particular location than to a specific house, as once that house has been demolished it will be reassigned to a new one at the same location.

The serial number at the butcher's is an example of a unique local number that has a very short life span. This number can be disposed of immediately after use. Important is only that two identical numbers do not occur at the same time in the queue.

Other numbers are temporarily unique for a longer period of time in a large geographical area. A car's chassis number, for example, must remain unique for a long period of time and requires a large geographical range. That number does not lose its significance until the car is scrapped. After a certain waiting period, the number could be re-assigned.

A temporary unique number is also sufficient in the area of immigration and naturalisation. For the period of time that a refugee stays in the Netherlands seeking asylum, the so-called alien number facilitates the registration of data and decisions. Ultimately, however, that person is granted Dutch residence and/or nationality or is forced to leave the country. The alien number can then be thrown away, even if one cannot exclude illegally staying on and re-applying for asylum. In order to prevent a rejected asylum seeker from illegal stay or re-applying, it is better to rely on fingerprint checking for recognition purposes than on a number.

Conversely, a BSN must last for longer than a person's life since confusion with the data of somebody else must be avoided for many years after a person's death. What is required for this is a permanently unique number that is not re-assigned to another person.

2.4 Number format

Numbers feature a wide range of formats. A telephone number in the Netherlands has ten positions, a BSN/SOFI-number nine. The number of positions required depends on the application. A number does not have to contain only digits, but can also hold letters. An apartment, for example, is often indicated with a combination of digits and a letter. Car registration numbers and chassis numbers in many countries are also alphanumeric. One of the advantages of letters in a number is that a position of a letter can have 26 different values, as opposed to that of a digit which only offers ten alternatives (0-9). Another advantage is that a number with a specific format containing digits and letters is usually easier to read and to remember than a number of equal length containing only digits.

2.5 Number semantics

Numbers often contain visible or hidden information (Blocksma & Van Maanen, 1990).

Many personal numbers make use of the date or year of birth, thus indicating the holder's age.

Those who know that the road network in the Netherlands is numbered clockwise from Amsterdam can use this concealed information to work out without much topographical knowledge that the A1 directly connects to Amsterdam, whereas the A27 does not.

The German car registration number indicates with the first letters the area in which the car is registered. The Dutch car registration number, on the other hand, contains a sequential national number system with six letters and digits, so that the number indicates the approximate year in which the registration number was issued.

Some numbers also contain a control digit to check whether there is anything wrong with the number. The BSN/SOFI-number, for instance, consists of 9 digits, the last of which is a control digit. To calculate that last digit, the first digit is multiplied by 9, the second by 8, and so on until the eighth digit which is multiplied by

2. The results of these eight multiplications are added together and then divided by 11. The digit that is carried after the division forms the ninth digit of the BSN. This control digit makes it possible to detect BSN-numbers that cannot exist, e.g. due to typing errors (Blocksma & Van Maanen, 1990, p. 87).

3 Legal aspects of number systems

This section discusses the legal position of a number system from the perspective of the European Data Protection Directive 95/46/EC that has harmonised the protection of personal data within the European Union. Keep in mind that there are often special laws applicable, too, such as - in The Netherlands - the Passports Act (e.g. in relation to the document number) or the Municipal Administration Act (GBA), regarding the administration number for residents, provided by that Act (the so-called A-number). Together, these govern the use of any number that can be traced to a person without making a disproportionate effort. In that case the lawful use of the number is subject to many conditions, with additional conditions if the personal number with its related data is legally defined as *sensitive* personal data, e.g. data containing information on a person's origin or race.
Number systems for legal entities, immovable property, objects, locations, transactions or events etc. are not subject to special data protection rules unless they qualify as personal data. To establish whether a number is a personal detail one should consider the application as a whole rather than looking only at the number itself. We therefore have to take account of all the surrounding technical, procedural and organisational provisions. A person whose real identity cannot be established without making a disproportionate effort is considered anonymous. If a personal number is kept anonymous within an application, no special protection or provisions for its use are required. Semi-anonymity (also called pseudonymity) is defined as there being at least one body that knows the identity of the personal number holder (e.g. the body that issued the number), while other users of the personal number cannot find out without making a disproportionate effort.

Subsections 3.1 – 3.8 below present a privacy law based policy framework for personal numbers or other numbers that in terms of data protection must be regarded as personal data in a specific application. The eight aspects discussed are: (1) purpose and purpose-restricted data-processing, (2) proportionality and subsidiarity, (3) delimitation of the target group, (4) voluntariness, (5) scale of application, (6) central versus decentral storage of numbers, (7) shielding and encryption of personal numbers and (8) independent supervision.

3.1 Purpose and purpose-restricted data-processing

The purpose of using personal numbers must be clear and known to all parties involved. The requirement of clarity and knowledge is in principle met in the case of use by (semi) public authorities if usage is provided for in a generally binding regulation. It is not permissible to collect and/or use personal numbers in violation of the current regulations. In assessing the legitimacy of an application, the balance of power between citizens and government - or between clients and companies - plays an important role. There is, however, also a grey area in which it is less easy to establish whether the application is legitimate. But unrestricted purposes are beyond doubt to be avoided. In principle, the use of a personal number should remain restricted to the original purpose of its registration. But the increase in identity fraud does however give rise to the question of whether processing control data to protect someone's identity against being stolen by another person, automatically makes this data-processing legitimate secondary use ('compatible processing') following the definition given by the Data Protection Directive, even if the control data were originally collected for a different purpose. May number administrators mutually compare their personal details related to the same person in order to detect identity fraud or to counteract the contamination of medical files with medical details of people other than the lawful holder of that citizen service number? The answer is probably yes if this is properly regulated and known to the person concerned. It is certainly yes if the person concerned has requested this protection himself.

3.2 Proportionality and subsidiarity

The use of a personal number system must be proportional, which means in reasonable relation to the purpose for which it is used. Subsidiarity means that if the objective can also be achieved in another, less radical way, that way must be given preference. The objective must, for example, justify the use of a personal number being compulsory; otherwise the number must be used voluntarily. Another example: a personal number should not be centrally stored if its objective can be equally well achieved with non-central storage on a chipcard in full control of the holder of the number. The subsidiarity requirement is also met by using a number with less far-reaching features such as a temporary number rather than a permanent one. Likewise, the subsidiarity principle implies that a general personal number should not be stated in full on an identity card but in a truncated way. With a copy of an identity card with the full BSN-number on it identity fraud would be too easy, while a truncated BSN 'xxxx3412x' (the control digit should not be shown) would be good enough for verification purposes. After all, the rightful holder can reasonably be expected to state the correct, full personal number if he sees this truncated number on his identity card.

Despite all restrictions applicable to personalised numbers, people generally opt for a personalised number, even if the purpose of the application would be equally well served with an anonymous or semi-anonymous number. Thus, the subsidiarity principle provides some room for improvement of our large-scale number systems!

3.3 Delimitation of the target group

The number system's target group must be clearly defined to be able to communicate with that target group and to determine the way in which the relationship between the parties involved is to be legally formalised. If the target group comprises the entire population of a country or a municipality, it makes sense to regulate the number system by legislation or (municipal) by-law. If, on the other hand, the target group consists of the personnel of a company or a shop's clientele, it will be appropriate to include regulation in a collective labour agreement/individual employment contract or in general terms and conditions, respectively.

3.4 Voluntariness

The use of personal numbers for private purposes is in principle permitted as long as people co-operate and voluntarily use their personal numbers. But when is co-operation truly voluntary? If a party occupies a monopoly position or a position of power, such as the government in relation to the citizen or an employer in relation to an employee, that co-operation cannot be regarded as completely voluntary. Not only these market conditions matter, the true freedom of choice can only exist if there is an alternative of equal value without the compulsory use of the personal number.

A party who issues or uses a personal number system will have to meet stricter conditions as the voluntary use of the number is less obvious. An example of such a condition is that the voluntary character must be attested to by the unequivocal, express permission of the personal number holder.

3.5 Scale of application

A large-scale general personal number is a likelier candidate for government supervision or regulation than a small-scale sectoral personal number because in case of a large-scale general personal number system the number holders' security and privacy are less controllable, and the chances of successful identity fraud greater. Small-scale applications involve less social risks (there can be more management control and the overall damage in absolute terms will be less). A small-scale sectoral personal number can also promote security and privacy if properly implemented and if there are some independently managed small-scale number systems with overlapping personal details that may be used to prevent identity fraud and errors. If this is the case depends on the type of number strategy in place, as we shall see in subsection 4.6.

3.6 Central versus decentral storage of numbers

The two extremes considered here are the storage of personal numbers with related personal data in a central database and non-central storage the numbers with related personal data being stored on a document or chip card issued to the holder only. 'Central' in this context means that all personal numbers and related personal details can be compared in a single run. The data can be physically stored in one place, but that is not necessary.

Using a central database in this sense makes it possible to carry out checks that would otherwise be impossible. With a central database one can, for instance, try to find out whether someone has already been included in the collection but under another number. One can also try to find out whether a number is registered in the name of more than one person (which is not the same as using someone else's personal number; this the centrally stored number's administrator cannot see without special monitor and verification tools).

The distinction between central and non-central is of legal significance because central storage involves more social risks, thus requiring a higher level of security. In the case of a specific application, the number issuing authority will have to compare the alternative solutions and find a reasonable balance between purpose and risks.

3.7 Shielding and encryption of personal numbers

The access to personal numbers and related data must be appropriately protected, and the level of security must be higher in keeping with the interest or value involved. From the security point of view, unauthorised access to and/or use of personal numbers must therefore be prevented, and traditional security measures must be in place, including encryption. This security requirement of the Dutch Data Protection Act differs from the requirement that the Dutch Penal Code sets for a punishable violation: a violation is only punishable if 'any security' shows that there was an intention to protect the number.

The shielding or encryption of a personal number deserves a special mention since there are new developments in this area that may have implications for large-scale personal number systems in the European Union. This concerns the Austrian model (Hayat et al., 2005). In this subsection 3.7 we look mainly at the shielding and encryption part of the Austrian model. It has also been shown to facilitate the interoperable use of different national personal numbers, so that e.g. each EU country does not need to issue its own personal numbers to residents of other EU countries and thus ultimately saddling all EU residents with dozens of different national personal numbers. We discuss this interoperability and its sector-specific derivation of disposable personal numbers, two other elements of the Austrian model, in subsections 4.1 and 4.2.

The Austrian model *(PIN—sourcePIN—ssPIN)*

In this model, the unique national personal identification number (PIN) is prevented from being taken outside of the central population register. Instead, from that PIN the central Source PIN Registration Authority derives a so-called 'sourcePIN' by adding a secret value to the secret PIN and encrypting the resulting number with the Source PIN Registration Authority's secret key. This sourcePIN is put on a Citizen Card issued to the holder only, in combination with the Source PIN Registration Authority's public key. If decryption using this public key yields a readable certificate, we know that the holder of the Citizen Card can be strongly assumed te be the right person and that we may trust the authenticity of the (hidden) sourcePIN on the Card, even though it is not possible to get hold of the sourcePIN itself.

For each public sector the Source PIN Registration Authority derives a sector-specific PIN (ssPIN) by adding the sector code to the sourcePIN and applying a one-way hash function to the result in a way that ensures that neither the original sourcePIN can be reconstructed from a ssPIN nor that ssPINs belonging to the same citizen can be traced back to each other. If authentication is properly done, this facilitates protected sector-specific online communication with and about the citizen, as well as administrative verification and data linkage (Hayat et al., 2005).

A sourcePIN is only stored in the Citizen Card of the rightful holder and remains the same during the holder's lifetime; the Source PIN Registration Authority is not allowed to keep a copy of a sourcePIN. In case a Citizen Card or ssPIN is compromised, the Source PIN Registration Authority can issue a new Citizen Card with a new set of ssPINs. The general idea underlying this shielding and encryption of personal numbers in the Austrian model is that in the event of loss, theft or other misuse it is possible to derive new sector-specific personal numbers without placing the original PIN or sourcePIN under threat. For that reason, sector-specific PINs are referred to as disposable personal numbers.

The Austrian model's protection of the original PIN and a sourcePIN derived from it provides a technical safeguard at the level of the personal number itself, a welcome addition to the current security measures at higher system levels, such as at the level of the personal number system as a whole (e.g. a password), the procedure (e.g. a transaction code) and the organisation (e.g. job separation).

3.8 Independent supervision

It can be desirable to have the management and the use of personal numbers supervised by an independent third party. This could be the Data Protection Authority or a so-called privacy-officer. Other options include an ombudsman or a trusted third party.

4 Number strategy

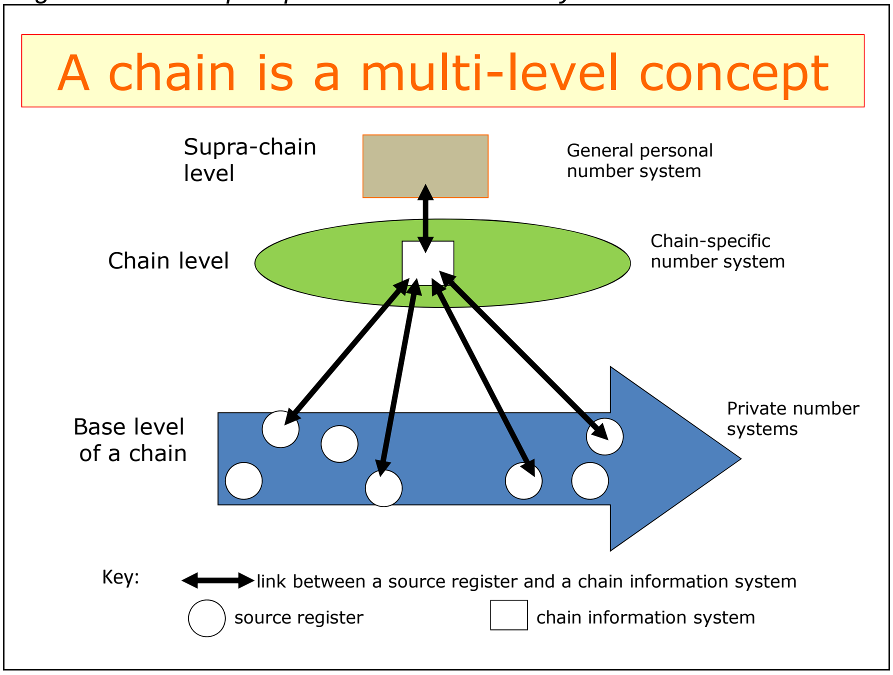
This section presents a number of strategic starting points for how a number system should be positioned and managed. We discuss seven issues related to number strategies: (1) positioning (vertical and horizontal), (2) chain linkage: the impact of a dominant chain problem, (3) multiple-chain usage of a number system, (4) number system management, (5) social effects of number systems, (6) type of number strategy: single, multiple or composite and (7) development patterns of number systems.

4.1 Positioning (vertical and horizontal)

4.1.1 Vertical positioning: at chain level, below or above

Figure 1 shows how number systems can be positioned *vertically* at three levels: (1) internal private number systems at the base level of a chain, (2) chain number systems at chain level and (3) general number systems at supra-chain level.

Figure 1. Chain perspective on number systems: three levels


A chain is a multi-level concept
Supra-chain level
General personal number system
Chain level
Chain-specific number system
Base level of a chain
Private number systems
Key:
link between a source register and a chain information system
source register
chain information system

A number system at the base level of a chain refers to a private number system managed by an organisation and used by one or more chain partners in their direct communication.

If the system is managed collectively on behalf of all organisations in the chain, independently of the individual chain partners' interests, a number system can be seen as positioned at chain level. Such a chain number system is part of the information infrastructure of a chain (Grijpink, 1997, pp. 89-109; 1999, pp. 33-35). It supports and steers information exchange in the chain.

General number systems are not chain-specific and can be used for many applications in many chains, national and international, depending on specific arrangements.

4.1.2 Horizontal positioning: interoperability

What should we do about similar numbers from other domains or countries? This strategic choice is important to the future of many national and chain-specific personal number systems in the European Union, whether it concerns the medical dossier, the criminal record or any other socially important area of European chain co-operation. Will residents of other EU Member States in the Netherlands be given a Dutch BSN for their relationships with the Dutch government, or will we opt for a system in which non-Dutch numbers can be incorporated? In that case we could describe the system as being interoperable, as demonstrated for the Austrian model (Hayat et al., 2005) by applying the PIN—sourcePIN—ssPIN transformation and their procedures to any foreign personal number (see subsection 3.7). Will a foreign patient be given a unique Dutch BSN, or will we opt for interoperability? This interoperability issue relates to the horizontal positioning of a number system. Although it might seem a governments' concern as the EU example demonstrates, any multinational company or any international chain co-operation can be confronted with this choice.

In the current situation, the Netherlands is opting for a non-interoperable system in which all foreigners with a relationship with the Dutch government will be assigned a unique Dutch BSN. That way, the stock of available national numbers will be exhausted at a faster rate and European citizens will eventually be burdened with a number of similar unique national personal numbers from any of the 27 EU-member states. Not to mention the multitude of other countries' sector or chain numbers.

The positioning of number systems is of strategic importance, because as the European integration is progressing the number of similar personal numbers for an average European citizen will grow tremendously.

4.2 Chain linkage: the impact of a dominant chain problem

In a barely manageable large-scale environment such as a chain, particularly a dominant chain problem can trigger interorganisational co-operation. In subsection 1.3 we introduced this chain perspective based on the theoretical framework of Chain-computerisation. Following this chain perspective, a number system is to be designed, implemented and managed primarily with focus on this dominant chain problem. For as long as a personal number system is absolutely necessary to the chain-wide co-operation to tackle the chain's dominant chain problem, there will be sufficient support for a common management of the number system in accordance with the requirements of that specific dominant chain problem. If a chain number is not or no longer necessary, the chain partners are not motivated to properly manage the chain number system and related personal data and actively combat misuse and fraud. The contamination of the chain number system and related data increases as its practicle value decreases. Ultimately, only a few chain partners will occasionally use the number system. In terms of the theory of *Chain-computerisation*, that number system has then lost its chain position, thus ending up at the base level of the chain.

A realistic chain concept contributes to our understanding of the difficulties and vicissitudes of large-scale number systems. It suggests that number systems should preferrably be chain-related. This chain linkage can be achieved in various ways, with as extreme variant using a number system that may not or cannot be used outside of a specific chain. Two other forms include the derivation of chain-specific PINs from an overall PIN as implemented in the Austrian model described in 3.7 or a chain-specific linking of a general personal number to a (any) chain-related personal detail. An example of the latter case could be the use of the Dutch BSN in the healthcare sector combined with an unvarying personal medical or physical characteristic (blood group and rhesus factor, for example). Any chain-specific detail will do as long as outsiders have to make a disproportionate effort to find out. This chain linkage is most powerful if the additional medical detail is regularly and carefully checked as a matter of course during the medical treatment, without that being considered an identity check! That way, someone's personal details are safely communicated or linked within the chain, while personal details of the same person from another chain cannot be directly linked. With this chain-specific variant of the BSN, misuse of somebody else's BSN cannot contaminate the medical files of both the official BSN-holder and the fraudster.
Finally, as we have already seen in subsection 3.1 on data protection for privacy,

chain linkage guarantees ligitimate ('compatible') data processing at chain level, if focused on tackling the dominant chain problem.

So, chain linkage is a good starting point for a personal number strategy.

4.3 Multiple-chain usage of a number system

This issue can best be explained with the example of the Dutch SOFI/BSN-number from subsection 1.4. Table 2 summarises its gradual development from confidential internal FI-number to compulsory general number in both the public and the private sector.

Table 2. Development of the Dutch SOFI/BSN-number

Policy area (ministry)	**Application**	**Notes**
Ministry of Finance	taxation, payment	confidential tax number until 1985, and then public
Ministry of Social Affairs and Employment	registration of employment, social security contributions, benefits and facilities	also used since 1988 by the social security sector
Ministry of the Interior and Kingdom Relations and Ministry of Transport, Public Works and Water Management	identity (SOFI-number on passport and driving licence)	also used by the identity chain since 1996
Ministry of Education, Culture and Science	school funding and other education applications	also used by the education sector since 2001
Ministry of the Interior and Kingdom Relations	identity (citizen service number on passport and driving licence)	the BSN has been the general personal number in the public sector since 26 November 2007
Ministry of Health, Welfare and Sport	medical patient file, medical data exchange	since 1 June 2008 the BSN has also been used as the unique personal healthcare number in this predominantly private sector

This example illustrates how tempting it is to adopt an already existing number in other chains as well. On the face of it, this appears to be an effective approach, but the (partly hidden) costs of shared use are often underestimated. This is because most people do not have a clear image of the increasing management problems and costs caused by multiple-chain usage. After all, a shared number plays a different role in each chain depending on the specific dominant chain problem. We will see in subsection 4.4 that this implies different levels of security that not every chain wants to accept because of the extra cost involved. Moreover, each chain is affected by different chain-specific sources of contamination. In the case of shared use, this leads to unexpected management problems, because people in the one chain have no idea of the specific contamination sources and forms of fraud in other chains and of the security measures in place. That results in an increasing amount of errors, while the gradually deteriorating quality of the shared personal number and related data in the various chains remains hidden until it is too late for easy remedies. At the same time, the broad usability of a general or multiple-chain personal number increases its economic or social value making abusing that number even more attractive, with the most chance of success in chains with a weak management variant. This is a self-reinforcing negative spiral. That is why a general or a multi-chain personal number system is difficult to manage.

> Example **Look-alike fraud with a general personal number**
> If someone identifies himself to his employer in the Netherlands with the driving licence of someone else who resembles him (known as 'look-alike fraud'), his employer also uses the BSN of the official holder of that driving licence for handing over to the tax authorities any withheld income tax and social security contributions. This way, the fraudster who has income from more than one source can evade additional income tax and the fraudster who is illegal and not entitled to work can prevent being arrested and expelled. The official holder of the misused BSN will have to pay additional income tax and fines because he seems to have failed to correctly declare his total income. Unless his protest succeeds, his fiscal and maybe his criminal record are contaminated.
> The fraudster although having paid his social contributions will be officially uninsured unless he – again – misuses somebody else's BSN, thus contaminating these medical and benefit files, too.
> A fraud in the identity chain thus has implications for tax collection, social security and health care that only come to light much later.

The adoption of an already existing number system usually throws up too many management problems. The starting point for a robust number strategy is therefore that number systems are to be chain-based and chain-specific, and that multiple-chain use is only advisable under special circumstances (see subsection 4.4).

4.4 Number system management

Contamination of number systems and related data or databases is not necessarily deliberate. Number systems become contaminated by usage, by changed circumstances and sometimes by the mere passage of time. Writing errors are virtually inevitable. Some details change in the course of time. An incomplete statement sometimes results in a second number being issued to the same person. A character set in an information system only using capitals or without diacritic marks (č, g, œ, ů, etc.), for example, leads to divergent spellings. Subsequent use of these spelling differences can result in details of a single person being erroneously registered under several numbers. On the other hand, if the holder of a personal number has an interest in obtaining a second number or linking his detail to somebody else's number, there are in practice many ways in which this can be elicited. Improper usage or misuse can in turn result in new incorrect registrations and links. In practice, each chain has its own specific temptations and opportunities for improper use or misuse of a number. Numbers with a high economic or social value are extra vulnerable.

The necessary characteristics, the desired reliability and the administration requirements of a number system are dependent on the chain process and the requirements set for that number by the specific dominant chain problem. Table 3 gives an impression of the varied requirements for the BSN system by the different chains using it. Based on this, we can identify various forms of management. In table 4 a distinction is made horizontally between passive and active management. The scope of the management activities is given vertically, from issuing a number to monitoring its use and actively fighting errors, misuse and fraud. That amounts to six different management regimes for number systems.

Depending on the entire application and value of the number, a chain features some general but also some chain-specific sources of contamination and forms of fraud. A number administrator can prepare himself for this by making use of all chain-related self-cleaning and self-resolving mechanisms. Generally speaking, people opt for the simplest and cheapest management variant that meets the requirements. Management variant 1, for example, is therefore generally adequate for a temporary chain number for objects, whereas management variant 6 is perhaps more appropriate for the management of a permanent public personal number with substantial social value.

Table 3. The citizen service number (BSN) in five social chains

Chain **Requirement**	**Tax matters**	**Social security**	**Identity**	**Education**	**Healthcare**
Purpose	registration, payment of tax	linking details and informal person recognition	linking details and informal person recognition	counting students	linking details and informal person recognition
Durability	duration of obligation to pay tax	period of a person's financialin-dependence	permanent and long after death	school period	permanent
Error tolerance	fairly high	fairly low	very low	fairly high	Extremely low
Risk of fraud	high	very high	high	low	fairly high
Damage	medium	fairly high	high	fairly high	very high

Table 4. Six management variants for number systems

	Passive	**Active**
Issuing	1 Allocation on request.	2 Allocation with legally-prescribed ID check based on documents and other data.
Administration	3 Registration of holder's details.	4 Registering holder's details, and periodically checking of the holder's rights, to prevent misuse.
Monitoring	5 Registering details about the use of the number and *registering* misuse or attempts at misuse.	6 Registering details about the use and registering misuse or attempts at misuse, and preventing and *combating* errors, misuse and fraud, before and after.

We are now able to define more clearly the adverse effects of multiple-chain use. Tables 3 and 4 showed that different chains set different requirements for a number and, accordingly, its management. Now that the citizen service number (BSN) is being used as a unique patient number in the healthcare sector, the very low error tolerance in medical chains calls for the most intensive management variant in table 4. The costs of this are in no way in keeping with the lighter management requirements in the tax and social security chains, where the adverse effects of extra fraud tend to be more rationally weighed up against the additional costs of fraud prevention. Because the propagation of errors and risks from one chain to another is difficult to predict or manage, the requirements of the most vulnerable chain should be applied for the management of a general personal number system in multi-chain usage. However, the support for the costs of this maximum management variant is often lacking in chains which themselves set less strict requirements. For this reason, in cases of multiple-chain usage one often settles for the minimum management variant, because this is being regarded as necessary by every number using chain. This has serious implications for the more critical or vulnerable areas of the number system application. Therefore, multiple-chain usage of a personal number can only be an effective number strategy if:

- the requirements of various chains or sectors are comparable
- the value of the number is barely increased by the multiple-chain usage
- the chain-specific sources of contamination are similar
- the knock-on effects of errors and fraud from one chain to another are reasonable predictable and manageable.

Only under those circumstances, the number system can be managed optimally for several chains at the same time. An example might be the multiple-chain use of a (new) sector-specific education number for these three chains within the education sector:

(1) the funding of schools; the amount of money depending on the number of pupils (= the number of education numbers),
(2) a national certificates registry, and
(3) the prevention of youngsters dropping out of the school system without a proper qualification.

Chain analyses should confirm that multiple-chain use of this (fictitious) education number system is adequate (Grijpink, 2010a).

Therefore, the key principle that number systems are chain-specific is related (among other things) to the ability to optimise management within the requirements of the chain. This key principle also implies that the multiple-chain usage of existing number systems will not usually be an effective number strategy.

4.5 Social effects of number systems (efficiency and privacy)

Two social effects of number systems are important within the scope of this article (Grijpink, 1999, p. 135): streamlining the exchange of information between autonomous organisations in a chain and enhancing the protection of privacy when processing or exchanging personal data in this chain. Compartmentalising the use of personal numbers with a view to protecting privacy is no less important than using numbers to prevent errors in chain communication. Therefore, both social advantages depend on the existence of chain numbers. As we shall see in subsection 4.6, that does however have implications for the use and management of general personal number systems.

4.5.1 Streamlining the exchange of information within a chain

Numbers are important to streamlining the exchange of information between autonomous organisations and professionals in a chain with the aim of structurally combating errors and chain failure. A number system at chain level makes it possible to administer essential – as seen from the dominant chain problem - personal details for all chain partners collectively, without those details having to be placed in every chain partner's internal source registers.

With a number system it is also possible to put in place a wide range of chain alerts, as described elsewhere (Grijpink, 1999; 2010b). The result of this is that the chain functions intelligently without each of the chain partners having to create large databases that cannot be kept up-to-date and if used repeatedly can lead to erroneous decisions.

4.5.2 Enhancing the protection of privacy

Secondly, number systems offer ways of enhancing the protection of privacy when processing and exchanging personal data. When using a number system in a chain's information infrastructure, the protection of privacy can be structurally enhanced in two ways:

a. by having personal data registered and exchanged in the chain using the chain's own number as much as possible, the ability of the chain's own employees to link these personal data to details from other chains is structurally reduced. If more than the chain's own number is needed for a certain action, these additional personal details can be retrieved from the chain number system. In the information society of the future, more attention will have to be paid to this *internal* protection of personal data. We are still concentrating too much on limiting and protecting the *external* exchange of data.

b. for communication between chains, the chain number of the demanding chain can be converted into the number of the chain on which the demand is being made, and vice versa. Numbers that are alien to the chain are thus prevented from spreading further, and the origin of a detail or a question can be screened off. If the criminal law enforcement chain wants to find out whether a detainee is receiving benefits, the enquiries to the social security sector must be made with the BSN rather than the criminal law enforcement number. If this number was visible to all authorised bodies in the social security sector, even if not involved in this particular case, everybody in that sector could see that the person in question was about to be imprisoned for a longer period of time (Grijpink, 1999,

p. 138). And that is precisely what the privacy regulations guard against.

Properly managed chain numbers are therefore a future-proof starting point for all large-scale, national and international number strategies.

4.6 Type of number strategy: single, multiple or composite

In this subsection we develop a starting point for choosing between a single, a multiple and a composite number strategy. A *single* number strategy is one that works exclusively with a compulsory general public number. A *multiple* number strategy is based on a lot of unrelated chain numbers. The *composite* number strategy combines these two number strategies.
However, as soon as the single and the multiple number strategies are combined, the synergy between the general and chain numbers begins to play a role. As is explained below, a composite number strategy for personal numbers is in fact conceivable, but not with a *compulsory* general personal number. So, choosing for a compulsory public general personal number blocks the way to any composite number strategy because the compulsory personal number drives out chain numbers.

Let us first take a more detailed look at the single and multiple number strategies.
If we have to choose between them, *a number strategy based on a lot of independent chain numbers* is preferable. After all, chain numbers yield the most flexibility of use and facilitate the effective management of each number system within the constraints of its chain. The advantages of chain-related self-cleaning and self-resolving mechanisms can be used to the full. The social or financial value for the holder is divided over several individual personal numbers, so that the value of each number remains low and each number is less vulnerable to misuse or attack. Chain numbers also facilitate streamlining chain communication (see subsection 4.5.1.) and protecting our privacy, at chain level and at the base level of a chain (see subsection 4.5.2). Chain numbers that are managed independently provide control information for quality assurance and identity fraud prevention.

Opposed to this multiple number strategy is the *single number strategy* with the compulsory use of a general public personal number in a wide range of situations, regardless of the chain processes being supported, and regardless of the problems being solved by this number system. A personal number system of this type, therefore, lacks a direct relationship with a dominant chain problem, so that chain-related self-cleaning and self-resolving mechanisms work less well. Making widespread use of the one general personal number increases its value, which makes it more vulnerable to attack, misuse and fraud. However, the available control information diminishes as chain numbers are replaced by the general personal number as the key to the related personal details. Thus, fewer independent chain number systems remain in place for quality protection and identity fraud prevention. At the same time, number management automatically seeks the lowest security level possible. Although the number management must – as we have seen – be directed at the most demanding chain that it serves, it is often the case that there is no support for the extra costs involved, so that in practice we make do with a minimum management effort.

The *composite number strategy* combines the advantages of both the single and the multiple number strategies. With the composite number strategy we make use of both independently managed chain numbers and more general personal numbers, based on agreed protocols for issuing, using and control. Number administrators can compare chain numbers with related data to verify whether the data are consistently linked to the right or the same person. That makes it possible to expose identity fraud or erroneous data links and to protect vulnerable data sets against contamination. For a general personal number to be used for this purpose we have to choose a number that will not harm or replace chain-related personal numbers. A *compulsory* general personal number is by law meant to replace other (chain) numbers, thus leaving us with a single number strategy! If the use of personal chain numbers is not permitted, the required management effort to maintain chain number systems will not be made. So, the composite number strategy can only be stable over a longer period of time if the use of the general personal number is not compulsory.

> Example **The Dutch model versus the Austrian model**
> The Dutch number strategy (May 2012) can be described as a single number strategy based on a compulsory general personal number, the BSN. However, the BSN can be overruled in a specific chain, but only if there is a statutory provision for the chain number preceding over the BSN. At the moment, this is the case in criminal law enforcement. So, in criminal law enforcement there is a composite number strategy in place.
> The Austrian model opts for a multiple number strategy based on a number of chain numbers (ssPINs) derived from the sourcePIN that cannot be related to each other. For government use only, the law provides for verification between the derived ssPINs in a secure environment within the government. The Austrian national personal number strategy can be considered a multiple number strategy; in the eyes of the government and the rightful holder of the Citizen Card the number strategy can be considered a composite number strategy.

The key principle here is that a complex information society calls for a composite strategy for personal numbers. The emphasis should be placed on chain numbers.

4.7 Development patterns of number systems

From Table 2 and 3 (see subsections 4.3 and 4.4) a development model of a number system can be derived which is presented in Table 5. This model follows the logical sequence of development stages of a number system from phase 1, in which it is used as an internal number by an organisation, to phase 7, with formal, public general usage, with collective, independent management.

Table 5. Growth path of a number system

Phase	**Scope of application**	**Functions**
1	internal use	registration
2	public number with chain usage, but without collective, independent management	an initially sheer administrative number develops into an informal tool to link data that relate to the same person or object and verify if this person is the right person, too
3	public chain number with collective, independent management	in this phase the administrative number develops into a formal key to relate data of the same person and to verify if this person is the right person
4	informal multiple-chain usage	a chain number is used informally by other chains, e.g. for verification (functions in the other chains as an 'internal' number, see phase 1)

5	formal multiple-chain usage	the number is officially adopted by another chain as its own number (see phase 3, the process repeats itself)
6	informal, non-public general usage, without collective and independent management	a number is used by authorised bodies as a general internal key to compare details supposedly related to the same person from several chains and to verify if this person is the right person
7	formal, public general usage, with collective and independent management	the number serves as a public, general key to data of the same person and can be shown on identity documents

The dynamic that ensures that a number system grows from the one development phase to the other arises mainly from the improper use and misuse of numbers and from the export of a number system to other chains. That is why the logical sequence of the development steps shown in table 5 is not often seen in practice. The interplay of forces results in a more zigzagging chronological growth pattern.

Phase 1: The internal use of number systems phase. An example of a phase 1 number system is the tax number when it was only used as an internal registration number for tax authorities and could not be retrieved.

Phase 2: This phase begins with the disclosure of a number, after which it is used chain-wide without there being a collectively managed chain-specific information infrastructure, a characteristic of phase 3. In phase 2 the number first functions as an administrative number, but it can gradually develop to an informal tool to link data that relate to the same person or object and verify if this person is the right person, too.

Phase 3: The third phase is typified by formal, public chain numbers. An example of this is the internet IP address system. That number system is collectively managed, independently of the individual interests of internet service providers (ISPs). The telephone number is another public number in phase 3, with (private) collective management. The Austrian ssPIN system fits within this phase.

Phase 4: This phase is characterised by informal multiple-chain use. The postcode-house number system is a number system with multiple-chain use, because it is informally used by other sectors for various purposes other than delivering mail.

Phase 5: Formal multiple-chain usage. This has been the case for the SOFI/BSN-number since 1988.

Phase 6: Informal general usage. The Netherlands already has some non-public, general number systems that are used as internal numbers for comparing details form several chains, such as the A-number of the Dutch municipal residents’ registry (GBA).

Phase 7: In this phase the number formally serves as a public, general key to related details of the same person and can be shown on identity documents. The Dutch citizen service number (BSN) has been in this phase since 2007.

5 A step-by-step plan for a number system

By way of a summary of the various aspects covered in sections 2-4, this section presents a ten-steps-procedure for the design, implementation and management of a (personal) number system. This checklist can also serve as a framework for assessing existing number systems.

1. What do the parties involved want to use the number system for? Which characteristics does the number system need (section 2: function, scope of application, unicity, number format and number semantics)? Benefit from the wide range of possible solutions so that the number can meet the requirements for a long period of time. Also consider easily transferable information in a number and the use of verification methods within the number to check for feasibility and to avoid writing errors. Do not opt for a permanent number if a temporary one is sufficient. If the number system must remain in place for a long period of time, take the increasing size of the target group into account, especially if it is meant to become a non-interoperable personal number system within the EU (subsection 4.1).

2. Is the number a number that will be considered a personal detail as seen from the application as a whole (section 3)? If not, there are no special legal restrictions. If so, can the number be used anonymously or pseudonymously? If so, these are the preferable options, a personalised number is not. If not, the requirements of privacy protection law apply (section 3: look separately at the various aspects). Notice that our privacy law set additional requirements for sensitive personal data. This is the case if the number contains, for instance, information about somebody's race or origin.

3. *Vertical* positioning (subsection 4.1.1) is at least possible at three different levels. If a number system can maintain itself at chain level in a stable manner, that positioning is preferable. The *horizontal* positioning (subsection 4.1.2) calls for a solution for similar numbers from other domains or countries. An interoperable setup is preferable for large-scale (national) personal number systems. If it is impossible to incorporate similar numbers from different domains or countries (compare the Austrian model), make sure that there are sufficient numbers, *also in the long term!*

4. Chain linkage is an important starting point for all number strategies (subsection 4.2). In which social chain must the number system play a role? Which role? Is the number system necessary to the chain-wide approach of the dominant chain problem? If not, consider an internal number system and have one of the parties manage that number system. If so, it is a public chain number. In that case, make arrangements for professional, independent chain number management. Given this chain's dominant chain problem, what requirements are to be met?

5. What type of management is required? In practice there are at least six different forms of management (subsection 4.4). Choose the simplest and least expensive form of management that meets the requirements. In this context, pay attention to the social and economic value of the number in the eyes of the holder and to chain-specific sources of contamination and types of fraud.

6. Can other number systems be used for verification and management? Develop an effective system to compare numbers. NB: this is not multiple-chain usage as meant in subsections 4.3 and 4.4, because one does not discard the chain's own number system.

7. Although chain linkage is a good starting point for *all* number strategies, consider sharing the use of an existing number system. Does a candidate number meet the requirements? Shared use of an already existing number can be preferred only if (subsections 4.3 and 4.4):

- the requirements of various chains are comparable;
- the economic or social value of the number is barely increased by multiple-chain usage;
- the chain-specific sources of contamination are similar;
- the knock-on effects of errors and fraud from one chain to another are reasonably predictable and manageable.

If in doubt, do chain analyses for every chain that will share the number system (Grijpink, 2010a). Be careful, because multiple-chain usage results in many additional management problems if these conditions are not met. Assess possible extra costs due to multi-chain usage and compare these costs with the costs of a dedicated chain number.

8. Number systems have two important social effects: they streamline chain communication and protect privacy (subsection 4.5). Does the application of the number system promote fast and accurate communication in the chain to tackle the dominant chain problem together? If not, develop some chain-computerisation solutions on the basis of the chain number (Grijpink, 1999, p. 19). Does the application of the number system in the chain promote the protection of privacy through registration and communication by number without additional personal data so that personal data are internally protected against misuse by employees? When enquiries are to be made in another chain, is the chain's own number replaced by the chain number of the other chain (and vice versa)? This way, people are less able to obtain information that they do not need to know.

9. A single number strategy appears to offer an inadequate basis for large-scale public personal numbers in a complex information society (subsection 4.6). Pay special attention to protecting the personal number by shielding and encryption (subsection 3.7; compare the Austrian model). Consider a composite number strategy, but make sure that using the general personal number is not made compulsory.

10. It turns out that there is certain logic in the development pattern of a number system (subsection 4.7). This can help in selecting or designing, implementing and managing a number system or developing a number strategy. Chain analyses have demonstrated that stepping back in the logical line of development is feasible, but that skipping a development phase will not usually meet with success at least not with regard to chain information infrastructures (chain analyses are being continuously published in the e-journal of Chain-computerisation).
http://jcc.library.uu.nl

Biographical notes: Jan Grijpink (1946) is Emeritus Professor, Utrecht University and senior advisor of PBLQ, IT consultants for government, in The Hague. Since October 2006 he has been chairing the Netherlands Biometric Forum (NBF). He is editor-in-chief of the e-Journal of Chain-computerisation. http://jcc.library.uu.nl

From 1995-2011 he was Principal Advisor at the Dutch Ministry of Justice, with a special focus on information strategy and identity issues.

He studied Economics (1969) and Law (1971) at Groningen University and earned a postgraduate degree in Organisation & Management Science (S.I.O.O. Utrecht) in 1976. In 1997 he obtained his doctorate at Eindhoven Technical University with a thesis about Chain-computerisation. He was appointed Professor in 2004 at Utrecht University.

Jan Grijpink regularly publishes on chain and identity issues in a complex information society focusing on large-scale information systems and chains.

References

Blocksma, M. & Van Maanen, H. (1990). *De Schaal van Richter en andere getallen.* [*Reading the numbers*.] Amsterdam: Bert Bakker.

Grijpink, J.H.A.M. (1997). *Keteninformatisering. Met toepassing op de justitiële bedrijfsketen. Een informatie-infrastructurele aanpak voor de communicatie tussen zelfstandige organisaties.* [*Chain-computerisation. Applied to the Criminal Law Enforcement Chain. An information-infrastructural approach to the communication between autonomous organisations.*] The Hague: Sdu Uitgevers.

Grijpink, J.H.A.M. (1999). *Werken met Keteninformatisering. Informatiestrategie voor de informatiesamenleving*. [*Chain-computerisation in practice. An information strategy for an information society*.] The Hague: Sdu Uitgevers.

Grijpink, J.H.A.M. (2000a). Chain-computerisation for interorganisational policy implementation. *Information Infrastructures & Policy*, *6*, 81-93. Amsterdam: IOS Press.

Grijpink, J.H.A.M. (2000b). Chain-computerisation for better privacy protection. *Information Infrastructures & Policy*, *6*, 95-107. Amsterdam: IOS Press.

Grijpink, J.H.A.M. (2002a). *Informatiestrategie voor Ketensamenwerking: Keteninformatisering als visie, resultaat en methode.* [*Information Strategy for chain co-operation. Chain-computerisation as perspective, result and methodology.*] The Hague: Sdu Uitgevers.

Grijpink, J.H.A.M. (2002b). Personal numbers and identity fraud: Number strategies for security and privacy in an information society (Part I and II). *Computer Law and Security Report*, 18 (5 and 6), 327-332 and 387-395. Oxford, UK: Elsevier Science Ltd.

Grijpink, J.H.A.M. & Prins, C. (2003). New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity. In C. Nicoll, J.E.J. Prins & M.J.M. van Dellen (Eds.), *Digital Anonymity and the Law: Tensions and dimensions*, pp. 249-269. The Hague: TMC Asser Press.

Grijpink, J.H.A.M. (2004). Identity fraud as a challenge to the constitutional state.

Computer Law and Security Report, *20*(1), 29-36. Oxford, UK: Elsevier Science Ltd.

Grijpink, J.H.A.M. (2006). Identiteitsfraude en overheid [Identity fraud and Government]. *Justitiële Verkenningen*, *7*(6), 37-57. The Hague: WODC/Boom Juridische Uitgevers

Grijpink, J.H.A.M. (2008). Biometrics security. Trend report on biometrics: Some new insights, experiences and developments. *Computer Law and Security Report, 24*(3), 261-264. Oxford, UK: Elsevier Science Ltd.

Grijpink, J.H.A.M. (2010a). Chain Analysis for Large-scale Communication Systems: A Methodology for Information Exchange in Chains. *Journal of Chain-computerisation*, *1*.

Grijpink, J.H.A.M. (2010b). *Keteninformatisering in kort bestek. Theorie en praktijk van grootschalige informatie-uitwisseling*. 2nd edition. [*Chain-computerisation in brief. Theory and Practice of large-scale information exchange*.] The Hague: Boom/Lemma Uitgevers.

Hayat, A., Posch, R. & Rössler, T. (2005). Giving an interoperable solution for incorporating foreign e-ID's in Austrian E-government. *Proceedings of IDABC-Conference 2005: Cross-Border e-Government Services for Administrations, Businesses and Citizens*, pp. 147-156. Brussels: European Commission. http://ec.europa.eu/idabc/en/document/3910/5803#proceedings.