Smart citizens wanted! How to act responsibly with data security and privacy?

Christine Ziske, Kikusema AB, Mariestad, Sweden
christine.ziske@kikusemamail.de
Ulf Ziske, KikuSema GmbH, Berlin, Germany
ulf.ziske@kikusemamail.de

Abstract:
The modern citizen is part of a worldwide digitalised system, in which (s)he is in a relationship with Third Parties, like, for example, e-commerce providers, Internet service providers, Trust centres and with the national government or other countries. The emerging concept of a Smart City requires a smart security, which is permanently evolving. This fact in turn requires smart citizens. The available resources of citizens when acting in their own interest cannot keep pace with the accelerated development of ICTs. Personal security will be reached by taking individual responsibility, by being the active party. We are convinced that only the competence of a human being is qualified to be a primary factor. But how to take responsibility? Today's authentication is based on Multi-factor Authentication (MFA) using combinations of passwords, software tokens, hardware tokens and biometrics. These currently available methods will be discussed and evaluated. The use of an eID is shown in different countries. As a user or consumer, one has to authenticate oneself several times a day. One has to use 'strong' passwords and is advised not to store these. Our concept 'Pass Sign' supports users in dealing with passwords or memorized secrets by augmenting their abilities. Thinking in patterns and remembering patterns is one part of human behaviour. Why not use a graphical interface by drawing an image on a virtual 'Compass Rose' and applying global things such as colours, directions, and patterns? Thereby, the ordinary keyboard with 94 characters can be replaced with a virtual key-board of the 65,535 characters from the UTF16 character set. The passwords are not stored at all. There is a demand for responsible action from all parties involved in the authentication process, including the citizen. That's why the citizen must be supported not only in the qualified use of passwords but also throughout the entire authentication process. The concept of the 'Five New Protocols' are aimed at improving the whole authentication process. Our concepts have the potential to be an innovative "survival kit" for smart citizens.

Keywords: human factor, graphical interface, authentication, memorized secrets, passwords, augmented intelligence

1. Setting the Scene

According to Sun Tzu: "Whoever defeats the enemy without battle really understands warfare" (Sunzi, 2011). We must bring together all the tools already available for strong authentication and secured processes in an easy but secure way to avoid breaches of citizens' privacy and property. The password is not dead despite many predictions and the variety of alternative solutions. Users need many different passwords. The average amount is about 100 to 200 accounts per user. It is difficult to find unbreakable passwords and keep them secure without writing them down. We are convinced that the human factor is an essential factor within the authentication process and needs to be supported and augmented by tools. Thinking in patterns is very typical and easy for humans. That was the basis for our work. In addition, we are convinced that there is a need to think in different ways instead of repeating the ideas of authentication already existing for decades.

2. Smart citizens of a Smart City

There is a variety of definitions of what is meant by a Smart City. The Smart City should meet new challenges in terms of services of general interest, the efficient organization of urban transport or the supply of energy as well as the ensured access to health care and education. To address these challenges information and communication technologies (ICT) should make an important contribution. The Smart City is a concept which links the major challenges of rapidly rising urbanization with the application of technologies to a vision of a sustainable city of the future (Beinrott, 2015). Today the Smart City concept is being tested and implemented by technology companies primarily in major cities around the world. The city is not smart but the people who live in it are smart. Smart citizens are not simply inhabitants of a Smart City. Eventually, it's about the optimal usage of technology by humans: "(…) the smart city is how citizens are shaping the city in using this technology, and how citizens are enabled to do so. "(Schaffers et al, 2012, p.99). The citizen should be considered as an active user of technologies and should be given appropriate tools to deal with these technologies. In addition to online banking or online trading, the smart citizen will be faced by many more topics such as Internet of Things, Cloud Computing, Spatial Data Infrastructure, Artificial Intelligence, and e-Government. In order to use all these offered services, one has to authenticate countless times a day. The number of accounts to authenticate and authorize has increased dramatically. The citizen must be empowered to meet these demands, because insecure authentication promotes cybercrime. The smart citizens need a smart booster to strengthen their own abilities.

3. Authentication today

3.1 Available solutions

The National Institute of Standards and Technology NIST (2011) states that living in a smart city based on modern ICTs puts citizens in front of the request to authenticate their digital identities to different parties many times a day. They must be able to utilize efficient, easy-to-use, and secure solutions.

Generally, the three factors, namely, knowledge ('something you know'), possession ('something you have'), and biometrics ('something you are') are the basis for authentication. Knowledge-based authentication are passwords or more precisely 'Memorized Secrets'. Memorized Secrets include passphrases and PINs as well as passwords.

"Authentication based on possession that means the use of One Time Passwords (OTPs) in the shape of hardware- and software tokens or the use of digital certificates based on Private Key Infrastructures (PKIs). The security of authentication is increased, but the use of PKIs is costly and time consuming" (Forst, 2014, p.7).

Biometric methods include the recognition of physiological characteristics as fingerprint, face, iris, palm vein, and DNS or behavioral characteristics as writing behavior, lip movement, voice, and gear.

Authentication by biometrics is based on the evaluation of probabilities and not sufficiently protected against facsimiles. Biometric characteristics contain more than the information required for authentication, e.g. on gender, ethnic origin or state of health. The utilization is a convenient way for citizens but poses risks of fraud and restriction of privacy.

Today's authentication is based on Multi-factor Authentication using combinations of passwords, software tokens, hardware tokens and biometrics. Very common is the usage of the smartphone as a possessing factor in combination with the use of different sensors, e.g. fingerprint scanner. As a result, the smartphone will become an exceptionally valuable item that has to be protected against misuse.

Governments around the world legitimize digital solutions called electronic identification (eID) to handle the authentication of citizens' identity. Apart from online authentication the option to sign electronic documents were given. The usage varies in different countries.

In Sweden, 97.5 percent of the population uses the Mobile BankID for authentication and signing in many areas of their everyday lives. The focus is on the access to e-government services, within the fields of tax, health insurance, pension fund or education. The spread in use is increasing within the private sector too, in online banking and especially for the cashless transfer of small amounts. "3.3 billion transactions were registered in 2018" (Wemnell, 2018, p.2). Since 2003 this type of eID has been available for PCs and since 2011 for mobile devices. In Austria, citizens are given access to public services online with a Citizen Card or Mobile Phone Signature. "Both alternatives can be used for providing evidence of identity and for the creation of legally valid signatures in online procedures. Numerous web services from both, the private and the public sector can be used e.g. tax assessment, insurance-data retrieval, criminal-record certificate, application for pension and child allowance" (Ziske, 2018, p33).

The German National Identity Card was introduced in 2010. It can be used for strong authentication on the Internet and to sign digital documents. Statista (2017) states that the number of users is below 15 percent. Only public services are offered. In the private sector, the eID is not used.

"In Estland over 90 percent of citizens file their tax returns digitally. Based on a Citizen Card practically every service, e.g. driver's license issue or parliamentary election can be handled electronically" (Deutschland Funk, 2018, p.1).

The mobile payment app from Alibaba as a kind of digital ID card is used by 520 million users in China. Other 980 million Chinese have linked their ID card with the WeChat account. Both should be usable in all situations, but unfortunately also for monitoring the citizens. (Corum, 2018)

Since September 2018, there is a European-wide recognition requirement for the various eIDs. In future, EU-citizens can use their own eID in other EU countries to enroll at universities, register their trade, submit tax returns or apply for vehicle registration. This is a good contribution towards supporting the global smart citizen, who does not always belong to the nationality of the city in which (s)he lives.

3.2 Evaluation

"The smartphone is becoming more and more the default device for Multi-factor authentication. It is used for receiving TANs by SMS or authenticator apps, for fingerprint or face recognition or as an NFC-device to detect additional hardware tokens, e.g. Citizen Cards. The price for the increased security is paid by the disclosure of your own telephone number" (Ziske, 2018, p.44). There is no anonymity anymore. The smartphone must not be lost, the phone number should not be changed. The increased protection reduces privacy. Furthermore, second factors of authentication are included without the consent of the user. The geolocation, specifically the IP address of a citizen is included as a second factor by Global Players, like Amazon, Facebook, and LinkedIn. Banks check typing behavior without user's agreement. The combination of behavioral and environmental factors is becoming more common. The legitimizing of eIDs by governments is a step in the right direction but the spread in all areas of life progresses too slowly. This is especially true in the private sector where ordinary logins with passwords only, are still in use. There must be solutions that work already today. There are only a few applications suitable for secure usage in a smart city. The use of the eID is combined with a PIN-code. PIN-codes are also passwords but composed of digits. This means the password is not dead. The password remains the controlling element. It means the citizen must be continually supported to handle the use of qualified passwords. Ordinary password manager or password vaults are not the solution because they require a master password.

How to handle this? Nobody can wait for the perfect final authentication infrastructures in a Smart City because the concept of a Smart City is already being introduced gradually. The citizen needs a 'survival kit' now to gradually improve authentication. The safest way of active participation is based on the cognitive abilities of human beings. That starts by using many different and complex password and time-limited passwords.

4. Boosting the Human Factor

An essential component is the 'human factor'; the conscious and intentional human act. That's a very controversial topic. It is important to consider whether and when the human factor should be included or excluded. We believe that security can only be achieved through the involvement of the persons concerned.

One of the six design principles for military ciphers stated by Kerckhoffs (1883) is:

it must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will.

These days this key is the password of a user. The access to user accounts and the protecting of data is usually based on password authentication.

The huge amount of attacks against passwords, like brute force (Kelley, et al., 2012), dictionary (Bonneau, et al., 2012) and social engineering makes it essential to use secure passwords. "At this point the user's ability to create 'secure passwords' came into the focus" (Bonneau, 2010, p.11).

A large range of studies have appeared on the subject of wrong or predictable user behaviour (Yan, et al., 2004; Taneski, Hericko and Brumen, 2014; Ur, et al., 2015) and how about choosing secure passwords (Schneier, 2014; Shay, 2014).

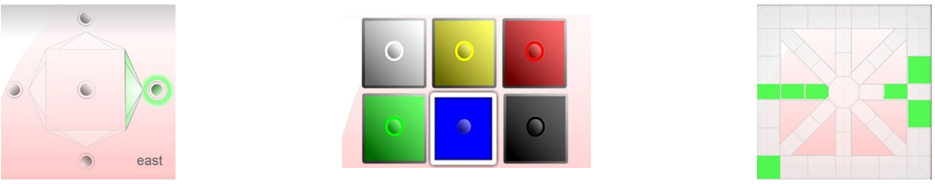
In addition, users need to cope with different password implementations at services on the Internet state (Horsch, et al., 2017). A lot of password requirements, which are fixed rules regarding password length and the allowed characters were postulated. These requirements are highly diverging between services (AlFayyadh et al, 2012).

Last June the NIST-Guidelines on secure passwords were completely revised. It is no longer talking passwords but 'Memorized Secrets'. Memorized Secrets should be interpreted to include passphrases and PINs as well as passwords. Now the user would have the option of assigning 64-character long passwords of any characters, including the space. The Memorized Secrets should be simple and easy to remember. For example, the password could be a sentence. And there is no need longer to change passwords regularly (Grassi et al, 2017). The new NIST-Guidelines on Digital Identities made some studies obsolete. (Bonneau, 2012) All this leaves the user in a real dilemma. Per se the user is completely on her/his own and needs practical help. Because we are convinced that the human factor and the Memorized Secret are the essential factors within the authentication process we were seeking tools suitable for supporting users and augmenting their abilities.

4.1 Boosting by the concept of the Pass Sign

What if there was the possibility to handle this huge number of logins or accounts in an easy way? The solution could be an innovative graphical interface with an extremely good memorability. An image only existing in the user's mind will be needed. The image is called Pass Sign. We've developed an application to implement this concept. The APP FabulaRosa provides you with complex and long passwords by drawing an image on a virtual 'Compass Rose' and applying universal things such as colours, directions, and patterns. The 'Memorized Secret' in the form of passwords is not stored at all; it is generated in the moment you draw the image on the screen.

4.1.1 FabulaRosa and Entropy



4+1 directions

6 colors

1 pattern/ max 45 button

Figure 1: FabulaRosa- Interface

You can choose 5 directions, 6 colours and 45 buttons that equals 30 levels.
30 levels by 45 buttons equals 1350 possibilities to activate a button. That represent a combination amount of 65,535 1350 = 1.7 $^{e+6502}$.
In other words, the extension of the Key Space, rather called Pass Space, is 65,535 with the power of 1350, which equals 1.7 with the power of e+6502. The entropy is 1,350*log2 (65,535) =21,599.9703.
The calculation is based on the work of Claude Shannon (Roch, 2009) who introduced the term 'Entropy' on the advice of John von Neumann as a mathematical criterion of the sufficient randomness.
"You should call it entropy. Nobody knows what entropy really is, so in a debate you will always have the advantage" (von Neumann, 1940/41).

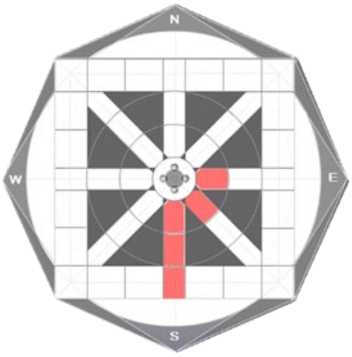
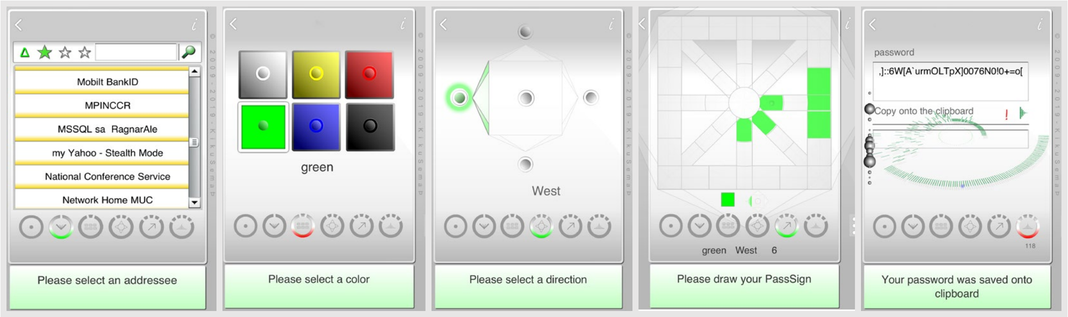


Figure 2: FabulaRosa - Pattern Interface



Mobilt BankID
MPINCCR
MSSQL sa RagnarAle
my Yahoo - Stealth Mode
National Conference Service
Network Home MUC

Please select an addressee

Please select a color

Please select a direction

Please draw your PassSign

password
.]::6W[A`urmOLTpX]0076N0!0+=o[

Copy onto the clipboard

Your password was saved onto clipboard

Figure 3: FabulaRosa – Screens of the app

4.1.2 FabulaRosa – What do you get

FabulaRosa provides regular passwords for ordinary logins as well as extremely long and complex passwords for high security applications. The passwords could have a maximum length of 850 with characters from the UTF16 character set which includes 65,535 characters. The passwords can be customized to requirements of the addressee that means the recipients of the login.

fhn1mkYXncfl9QAAZApgs9akxW9vAp5AJ2LoMqA
h1wAjMOAjVbS7yAuvW4RwEqsc

斎刲昙讟淂鲲奢乖三京淨民丨蛳亩嫷

[illegible]
[illegible]
[illegible]

Figure 4: FabulaRosa – Examples for passwords

4.1.3 FabulaRosa – What are the Algorithms behind

Behind the layout of 'FabulaRosa Engine' is a hidden universe, enriched with a so-called Pass Space with 1350 spheres. Each addressee has its own universe. The FabulaRosa Algorithm can be used for creating passwords and for encryption. The FabulaRosa Algorithm represents the engine of the whole concept and consists of the following parts.

- *The Pattern You Draw – The Pattern*
  You can select 45 buttons, 6 colours and 5 directions. 6 colours by 5 directions that equals 30 levels. 30 levels by 45 buttons equals 1350 possibilities to activate a button. All buttons are linked with each other and each button correlates with a so-called *Mass Number*.
- *The Addressees You Allocate – The Mass Number Algorithm*
  A so-called *Alias Addressee* is created for each addressee. The Mass Number will be calculated by a certain algorithm based on this Alias Addressee.
- *The User You Are*
  Each user has its own so-called *Individual Security Constant* which ensures that two users using the same <pattern> will NOT use the same <password>.

The user gets an individual key set. These keys are transformed into the Individual Security Constant.
The password is calculated with a length of 1350 characters using the UTF16 character set.
The password is customized to the requirements of the addressee regarding the feasible length and the character set.
The whole app can be protected against unauthorized access by the so-called *Safety Start Algorithm*.
The entire user data, including all the information about the addressees are encrypted. One can't proceed within the app without drawing an additional pattern.

5. Boosting the whole authentication process

The boosting of the Human Factor needs to be extended from qualified use of passwords to mastering the entire authentication process. This must be done qualitatively and quantitatively. The smart citizen will be faced by more and more parties. Perhaps the construction of a Smart City will soon resemble the Tower of Babel. By analogy, the different languages are now the different security services. Our general point of view is that the user has to be self-reliant concerning using modern technology. Today's authentication via smartphones becomes more and more essential for the user, both in private or public spaces, whether using trustworthy or untrustworthy devices. But how to handle authentications issues in unsure public environments and how to enforce the entire authentication process? Furthermore, the objective should be that the unauthorized access to users' sensitive data does no longer lead to serious consequences. How to realise that? Users' sensitive data must be stored and transmitted only with encryption. Each privacy data value must be encrypted by itself. The use of Memorized Secrets must be time-based otherwise the authentication process will be blocked.

5.1 Boosting by the Five New Protocols

The following are Five New Protocols:
Protocol 1 – QR Code
Protocol 2 – Stealth Mode
Protocol 3 – Secret Based Login
Protocol 4 - Encrypted User Data
Protocol 5 – Multi Instance Authentication/Scrambled Secrets

These were developed to overcome current issues within the authentication process.
Firstly, because passwords can be intercepted and cracked the Stealth Mode was developed.
Secondly, because the addressees, e.g. web hosts probably protect user credentials insufficiently, sensitive data can be misused. That's why the idea of transferring 'content free strings' was born. Finally, there is a need to overcome the so-called Keyhole Security which means only locking the door of your safe by using a simple 'True-False-Authentication-Mechanism'.
There is the problem of authentication in public spaces with untrusted devices. This problem could be solved by Protocol 1. Between personal smartphones and public devices, a password is transferred by QR-Code.
By using Protocol 1 the real password or its hash is transferred. This disadvantage is solved by applying Protocol 2, the Stealth Mode. The password is changed within a certain frame so that it cannot be identified during the valid period.
With Protocol 3 the attack of the password transfer is avoided. Only a 'content-free string' will be sent to the user. During the handling of the login by the engine of FabulaRosa the string will be scrambled.
Protocol 4 enables the user to encrypt and decrypt complex data locally by using the engine of FabulaRosa. Complex data could be users' sensitive data, files, and applications.
The idea behind Protocol 5 or Scrambled Secrets is protecting your 'values' themselves by encrypting. This can be combined by using a Multi-Instance-Mode. Up to eight instances which could be a mixture of different technical factors with different simultaneous authorities can be involved in the process.
These protocols were already developed in 2010. Only the QR-Code is used by many users in different apps. The mass of data breaches has not caused service providers on the Internet to introduce real innovations, such as the 'Stealth Mode'. The concept of 'content free string' can improve the Cloud security. Most users' sensitive data is kept carelessly and not even encrypted in the providers' clouds. Scherschel (2019) states recently that trivial vulnerabilities in five of the world's largest web hosts endanger the users' credentials of 7 million domains. If the data only makes sense when converted back by the user, the hackers will not be able to exploit the intercepted data.
Innovations are being hesitantly introduced. The change of mindset and its implementation is an even more cumbersome task. Innovations must prevail against the 'sluggish user' who prefers simplicity rather than security. It is not easy to put Sun Tzu's principles of being proactive into practice.

The following figure illustrates firstly the status of the implementation and that the security level will increase from protocol to protocol.
Secondly, it shows that the security level increases as the user participates more actively and/or third parties, like cloud service provider, web hosts or e-Government services invest in securing the entire authentication process.

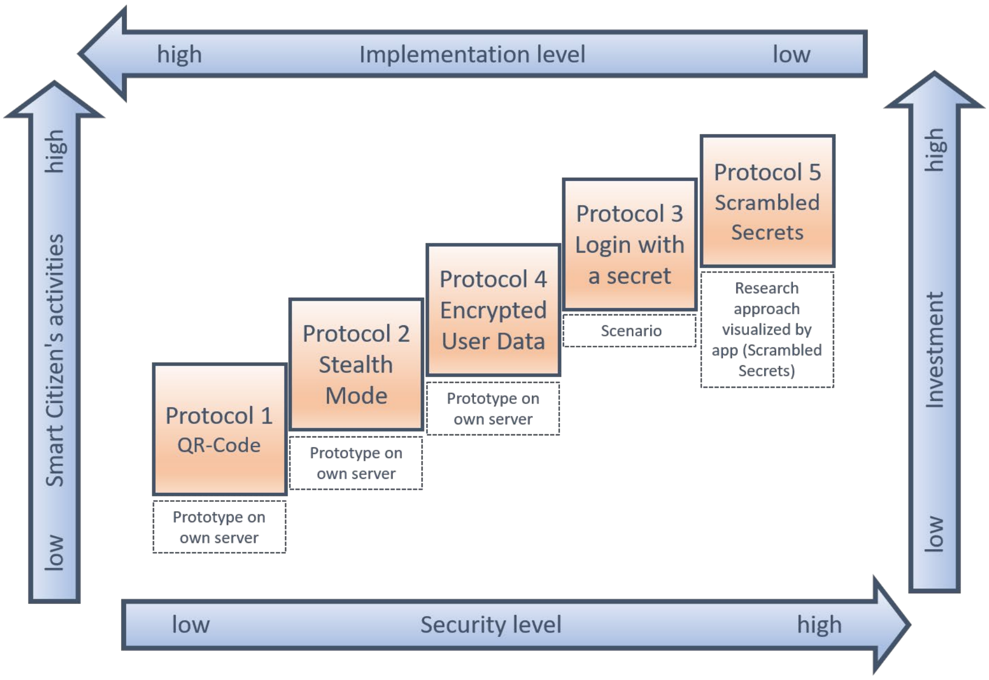


Figure 5: The Five New Protocols

6. Conclusions

The vision is to create a ‘citizen-centric authentication system` in which personal data is handled securely by using solutions which will be Ease-of-use but making it more difficult for criminals to compromise online transactions. The citizens must have the confidence that their own digital identity, privacy and property is adequately protected.

The citizen must have the trust in the Smart City and all its technical and organizational components. Just as one climbs into a plane or a lift with the confidence that it will not crash. The complexity of the technical systems and the individual interests of all smart citizens must be considered.

Several authentication methods were offered today. Smartphones are often used within Multi-factor authentication methods or for the handling of eIDs. Biometrics and behavior are increasingly involved at the risk that privacy is infringed. Most of these solutions are dependent on the finally use of PIN-codes or, at best on Memorized Secrets.

The knowledge-based factor ’something you know` remains the determining factor of authentication.

We are aware that the human factor is both – the weakest and the strongest link in the chain.

But we are convinced that only the competence of a human being is qualified to be the primary factor in authentication and that the human factor has to be strengthened. Personal security will only be reached by taking individual responsibility, by being the active party.

Our concepts of ‘Pass Sign’ and ‘The Five New Protocols’ will empower the smart citizen to act responsibly with data security and privacy.

Our vision is that once adopted, our concepts and apps can help to assure that security, privacy, interoperability and ease of use will be significantly improved for all parties, which are involved in the authentication process. We are looking for committed partners to walk together on this path.

The News Needs Friends!

References

AlFayyadh, B., Thorsheim, P., Jøsang, A. and Klevjer, J. (2012) Improving usability of password management with standardized password policies. In *Proceedings of Sécurité des Architectures Réseaux et Systèmes d'Information*, Cabourg.

Beinrott V. (2015) Bürgerorientierte Smart City Potentiale und Herausforderungen. [online]
Available at: <https://www.zu.de/institute/togi/assets/pdf/TOGI-150302-TOGI-Band-12-Beinrott-Buergerorientierte-SmartCity-V1.pdf> [Accessed 16 December 2018].

Bonneau, J. (2012) The science of guessing: analyzing an anonymized corpus of 70 million passwords. In: *Proceeding of the IEEE Symposium on Security and Privacy*. San Francisco, 2012, IEEE. pp 538–552.

Bonneau, J., Herley, C., Van Oorschot, P.C. and Stajano, F. (2012) The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In: *Proceeding of the IEEE Symposium on Security and Privacy.* San Francisco, 2012, IEEE. pp 553–567.

Bonneau, J. and Preibusch, S. (2010) The password thicket: technical and market failures in human authentication on the web. In: Proceedings of the Ninth Workshop on the Economics of Information Security *(WEIS*) Cambridge, 2010.

Corum, C. (2018) *Chinese digital ID comes to Alibaba's payment app.* [online] Available at:
<https://www.secureidnews.com/news-item/chinese-digital-id-comes-to-alibabas-payment-app/?tag=email>
[Accessed 11 June 2018].

Deutschland Funk (2018) *Zwischen digitaler Moderne und Sowjetvergangenheit*. [online] Available at:
<https://www.deutschlandfunk.de/estland-zwischen-digitaler-moderne-und-sowjetvergangenheit.724.de.html?dram:article_id=408828> [Accessed 13 July 2018].

Forst, C. (2014) *Sichere Authentifizierung – Teil 1: Klassische Methoden*. [online] Available at:
<https://conplore.com/sichere-authentifizierung-teil-i-klassische-methoden> [Accessed 29 November 2018].

Grassi, P.A., Fenton, J.L., Newton, E.M., Perlner, R.A., Regenscheid, A.R., Burr, W.E. and Richer, J.P. (2017) *Digital Identity Guidelines. Authentication and Lifecycle Management*. (NIST Special Publication 800-63, Version 1.0.2, pp 13–15) [online] Available at:
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf> [Accessed 10 August 2017].

Horsch, M., Braun, J. and Buchman, J. (2017) Password Assistance. In: *Proceedings of Open Identity Summit.* Bonn: Köllen Druck+Verlag GmbH., 2017.

Kelley, P.G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor L.F. and Lopez, J. (2012) Guess Again (Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms. In: *Proceeding of the IEEE Symposium on Security and Privacy.* San Francisco, 2012, IEEE.

Kerckhoffs, A. (1883) La cryptographie militaire. *Journal des Sciences Militaires.* 9, pp.5–38 & pp.161–191.

NIST: National Institute of Standards and Technology (2011) *National Strategy for Trusted Identities in Cyberspace, Enhancing Online Choice, Efficiency, Security, and Privacy* [online]
<https://www.nist.gov/sites/default/files/documents/2016/12/08/nsticstrategy.pdf> [Accessed 21 December 2018].

Roch, A., (2009) *Claude E. Shannon: Spielzeug, Leben und die geheime Geschichte seiner Theorie der Information*. Berlin: Gegenstalt Verlag.

Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Tsarchopoulos, P., Posio, E., Fernandez, J., Hielkema, H., Hongisto, P., Almirall, E., Bakici, T., Lopez Ventura, J. und Carter, D. (2012), *Fireball - Landscape and roadmap of future internet and smart cities*. [online] Available at: <https://hal.inria.fr/file/index/docid/769715/filename/FIREBALL_D2.1_M24.pdf> [Accessed 3 January 2019].

Scherschel, F. (2019) *Triviale Hoster-Sicherheitslücken gefährden 7 Millionen Domains*. [online] Available at:<http://www.heise.de/-4275552> [Accessed 4 January 2019].

Schneier, B. (2014) *Choosing secure passwords* [online] Available at: <https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html>[Accessed 23 March 2018]

Shay, R., Komanduri, S., Durity, A.L., Huh, P.S., Mazurek, M.L., Segreti, S.M., Ur, B., Bauer, L., Christin, N. and Cranor, L.F. (2014) Can long passwords be secure and usable? In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '14. New York, NY: ACM, pp 2927–2936. [online] http://doi.acm.org/10.1145/2556288.2557377.

Statista (2017) *Für welche Zwecke haben Sie die Online-Ausweisfunktion des neuen Personalausweises (nPA) bereits eingesetzt*?, [online] Available at: <https://de.statista.com/statistik/daten/studie/777662/umfrage/nutzung-der-online-ausweisfunktion-des-npa-in-deutschland/> [Accessed 5 January 2019]

Sunzi. (2011) *Die Kunst des Krieges*. Translated by H. Eisenhofer. Hamburg: Nikol Verlagsgesellschaft.

Taneski, V., Hericko, M. and Brumen, B. (2014) Password security – No change in 35 years? In: *Proceedings. 37th International Convention on Information and Communication Technology, Electronics and Microelectronics MIPRO.* Opatija*,*2014*,* IEEE.

Ur, B., Segreti, S.M., Bauer, L., Christin, N., Cranor, L.F., Komanduri, S., Kurilova, D., Mazurek, M.L., Melicher, W. and Shay, R. (2015) Measuring real-world accuracies and biases in modeling password guessability. In: USENIX, *Proceedings of the 24th USENIX Security Symposium.* Washington, D.C*.,* 2015*.*

Von Neumann, J. (1940/41) Conversation, between John v. Neumann and Claude Shannon, occurred between fall 1940 to spring 1941 at the Institute for Advanced Study, Princeton, New Jersey. [online] Available at: <http://www.eoht.info/page/Neumann-Shannon+anecdote> [Accessed 01 May 2018].

Wemnell, M. (2018) Statistik BankID – användning och innehav – fördjupning. [online]Available at: <https://www.bankid.com/assets/bankid/stats/2018/statistik-2018-12.pdf> [Accessed 13 December 2018].

Yan, J.J., Blackwell, A.F., Anderson, R.J. and Grant, A. (2004) Password Memorability and Security: Empirical Results. *IEEE Security & Privacy*, 2(5), pp 25-31.

Ziske, C. (2018) Ist das Passwort tot? Sichere Authentifizierungsverfahren.
Lecture at DITACT women's IT Studies, Salzburg 20th August 2018. [online] Available at: <http://ccc.ziske.de/wp-content/uploads/2018/08/9Password_ditact2018.pdf> [Accessed 19 December 2018].