BankID and two-factor authentication.

Anders Kofoed
anderkof@stud.ntnu.no
TTM4137 Wireless Security Technical Essay

November 20, 2013

1 Introduction

Security in the world of e-commerce is an important issue. The Norwegian banking community has developed an solution called BankID, utilising a PKI and two-factor authentication. The idea behind BankID is to make a national identification system, providing authentication as well as digital signatures. BankID is used as the main authentication service in most online banking sites in Norway. The implementation is fairly similar to other known security systems, with some differences worth looking at. This essay will explain how the system is built, focusing on the main architecture and the two-factor authentication process. Towards the end I will briefly discuss some of the challenges faced by the project.

2 Problem Discussion

2.1 Components and Architecture of the BankID system.

PKI, public key infrastructure is the preferred model for efficient and secure online services. Often accompanied by the use of several factors of authentication. PKI is a widely used technique used to provide public encryption and verification(digital signatures). The normal way of implementing a PKI, is by supplying each entity with their own private key, which only they have control of. Then distribute the corresponding public key used to verify signatures and encrypt data. BankID simplifies this structure by storing the signing keys centrally, as well as doing all the cryptographic function on the central server. In other words, no software or sensitive information is stored on the users' computer. An overview of the architecture is displayed in figure 1 [2]. We can divide the components shown into two main parts, a central infrastructure and a distributed part. The central infrastructure consists of storage databases for certificates, cryptographic keys, all the bank's CAs, the validating authority and interfaces towards end-users and merchants. The distributed part, involves the BankID server, and the client running in the user's browser. We also see a RA (registration authority),

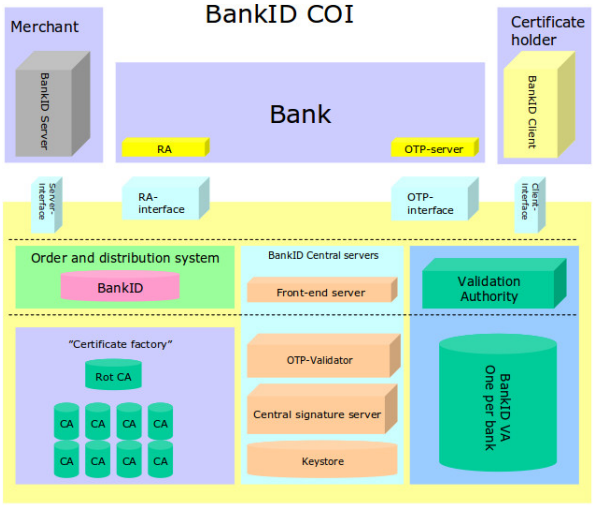

Figure 1: BankID architecture.

which is implemented in the banks' internal systems. This entity is used when a new user wants to obtain a certificate, thus registering with the central interface [3]. When either entity (user or merchant) wants to sign or verify something, he must authenticate with the central infrastructure where the crypto is carried out.

Two-factor authentication is used to obtain mutual authentication between the BankID client and server (user and merchant). When performing authentication, the goal is to prove that you are who you claim to be. This is done using one or more *factors* of authentication. The three basic factors used in authentication is: [1]:

- A secret the user *knows*, typically a user generated password/PIN.
- Some device or secret the user *has*, examples are the smart card piece of a normal visa card or password generating tokens.
- Something the user *is*, such as fingerprints, handwriting recognition or keystroke rhythm recognition.

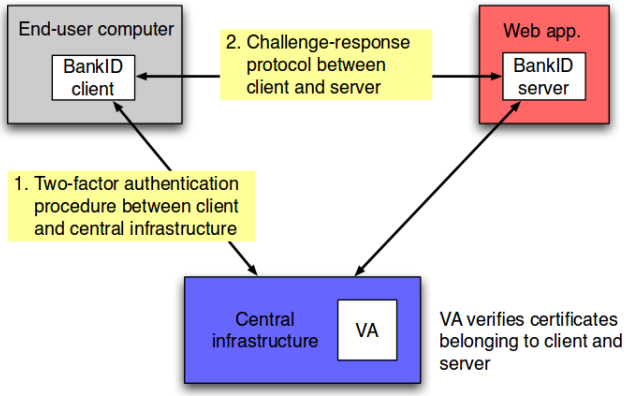

Figure 2: BankID authentication procedure.

The whole authentication procedure between client, server and the third party is shown in figure 2 [3]. First the user enters his social security number which is used to generate a list of the users associated BankIDs (it is possible to have several). Then the client prompts the user for a one time password (OTP), generated by a password-generating token issued by the bank. This OTP is then verified at the central infrastructure, assuring the authenticity of the user. Next a static password is entered, which is used as a passphrase to gain access to the cryptographic keys [1]. Now the private keys can be used by the infrastructure to authenticate with the server on behalf of the user.

The procedure described is a classic two-factor authentication process, with the factors being the OTP and the static password. Using two or more factors mitigates the problem of password getting stolen, or replayed by attackers.[5] Usually the OTP device generates passwords which either change over time, or has a counter used to synchronise with the validator. If one of these passwords is stolen, they wont be usable for the attacker, since it only can be used once. Newer systems has now started to look at mechanisms enabling the use of mobile phones as password generating tokens. The password generating functions is implemented in the phone, with all the factors needed to generate the OTP stored in the phone and on the server. Factors such as identification number (IMSI or IMEI), timestamps (hour, minute, day) or other pseudorandom metrics are used when generating OTPs [6].

2.2 Security Capabilities

The primary objective of the system is to enable two parties without a trusted relationship to establish a secure communication channel. We see (in figure 2) that the establishment of the channel is done through a third party, which both communicating parties trust. This third party is the central infrastructure operated by BankID. The public-private key pair is generated by

this entity on request from the banks. The private key is stored in the central database, while the public key is stored at the CA related to the customer's bank (may also be in the central infrastructure). When a user wants to use the BankID client, a Java applet is downloaded in the browser. The user is advised to check the certificate of this app, to assure the authenticity of it, and avoid phishing attacks. The user then authenticates with the server, and gives the central infrastructure access to the stored keys. Next, the infrastructure executes the actions requested (e.g. signing a challenge or a document). The BankID server, being online stores or similar merchants can then verify the signed challenge received from the client and vice versa [4] [3]. The two parties have now established a mutually secure relationship. This procedure have to be done every time a user wants to carry out transactions with the merchant. I.e. when doing online banking, the user has to first authenticate when logging in, and then again when confirming a transfer. This makes it less desirable to hijack sessions, because the system will require more OTPs to complete account transfers.
A guidance entitled *Authentication in an Internet Banking Environment* [1] was issued by the Federal Financial Institutions Examination Council, 13th September 2011, emphasising the importance of risk assessment when working within the internet delivery channel. The guidance argue that the only adequate authentication mechanism when dealing with high-risk transactions is multi-factor authentication.

2.3 Challenges and Vulnerabilities.

There are can choices in the design that can be questioned. One fundamental requirement when using PKI systems, is that the user should be in control of their own keypair [7]. Storing these in a server would - in a worst case scenario - open for an insider attack, since the banks is in total control of the users keys and certificates. There are some publications displaying attacks on the BankID system, but the banks claim to have fixed all of them. These attacks include man in the middle attacks, where the attacker sits between the customer and the infrastructure or BankID server. This attack exploits the assumption by the banks that users always check the certificate of the java application, which most users does not do. After tricking the user into authenticating with a fake app on a "MITM-server", the attacker relays the traffic until the authentication is completed. If the attacker wants to transfer money from the user's account, he will need one more OTP. This can be obtained by alerting the user that the first one was wrong, thus trick him into entering one more [8]. This attack is most likely not feasible any more, but problems with the use of forms and web applications are still relevant.

3 Conclusion

Dealing with high risk transactions involving sensitive user data and especially movement of funds, demands security on the highest level. I think that a move towards a more user controlled system would benefit all parties involved. Using two or more factors when authenticating is the best way to go, but it is mostly necessary because the user credentials is saved centrally. If keys and functions were to be moved to the users' phones (as proposed by BankID in [9]), it would be interesting to see if key-generating tokens still would be used. This alternative allows users to sign and authenticate without involving a third party. If this was to become the standard, new problems would surely arise, but it is an interesting alternative to consider.

References

[1] Federal Financial Institutions Examination Council *Authentication in an Internet Banking Environment* 13-Sep-2011 http://www.digitallibrary.kcci.com.pk/handle/32417747/701

[2] Bankenes BetalingsSentral AS *BankID COI White Paper* 05.09.2005 http://www.eurim.org.uk/activities/pi/BankIDWhitePaper.pdf

[3] Professor K. J. Hole, Department of Informatics, University of Bergen *Next Generation Internet Banking in Norway* https://bora.uib.no/bitstream/handle/1956/2636/Dr.Avh._Thomas_%20Tjostheim.pdf?sequence=1#page=141

[4] IEEE SECURITY & PRIVACY *Secure Internet Banking Authentication* The IEEE Computer Science, March/April 2006 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1621056

[5] B. Schneier, *Two-Factor Authentication: Too Little, Too Late.* AprilRisks 02.18.2005. http://www.itsec.gov.cn/webportal/download/2004_two-factor.pdf

[6] Fadi Aloul, Syed Zahidi, Wassim El-Hajj, *Two factor authentication using mobile phones,* Computer Systems and Applications, IEEE/ACS International Conference on Computer Systems and Applications, 2009 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5069395

[7] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures *Official Journal L 013 , 19/01/2000 Article 2* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:HTML

[8] NoWires Research Group, Department of Informatics UiB *A Proof of Concept Attack against Norwegian Internet Banking Systems* Short paper version, Feb. 21st, 2008.

[9] BankID Norge *BankID p mobil* (In Norwegian.) https://www.bankid.no/Dette-er-BankID/BankID-pa-mobil/ Read 19.11.13