Jerzy PEJAŚ, Tomasz KLASA
WEST POMERANIAN UNIVERSITY OF TECHNOLOGY, FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
ul. Żołnierska 52, 70-210 Szczecin

Identity verification based on certificateless public key cryptography

Ph.D. eng. Jerzy PEJAŚ

Assistant professor at the Faculty of Computer Science and Information Technology of the West Pomeranian University of Technology, director of Information Security Team, specialist in Public Key Infrastructure (PKI) and PKI services, applied cryptography methods, vulnerable information access nd authorization systems and technical and legal problems of digital signature.

e-mail: jpejas@wi.zut.edu.pl

Ph.D. student Tomasz KLASA

PhD student at the Faculty of Computer Science and Information Technology of the West Pomeranian University of Technology, author and co-author of a number of articles and book chapters in the area of risk management and information security.

e-mail: tklasa@wi.zut.edu.pl

Abstract

Verification of claimed identity becomes a problem of growing significance nowadays, as the number of e-commerce transactions grows rapidly and new information distribution channels are created by companies and institutions of all kinds. As most of them rely or make a use of a public network, such as the Internet, security of transferred data and information in most cases requires authorization of the user. Unfortunately, most existing authentication solutions create rather weak binding with real identity of the user, while some, like ID documents, are worthless in case of electronic transactions as they are nothing more than just a piece of paper or plastic, with no real connection with the electronic system. A secure digital signature based on traditional PKI, at the same time, relies on trust migrated through commercial companies, with the help of certificates. The proposed protocol of identity verification combines national e-ID document functionality with certificateless Public Key Cryptography (CL-PKC) to provide a safe and trustful way of identity verification, joining most advantages of current systems and limiting downsides to a minimum.

Keywords: identity verification, authentication, information security.

Weryfikacja tożsamości oparta o bezcertyfikatową kryptografię klucza publicznego

Streszczenie

Weryfikacja tożsamości stała się problemem rosnącej wagi, gdy liczba transakcji w handlu elektronicznym rośnie gwałtownie a nowe kanały dystrybucji informacji są tworzone przez różne firmy i instytucje. Ze względu na fakt, że większość z nich wykorzystuje sieć publiczną, jak na przykład Internet, bezpieczeństwo przesyłanych danych i informacji w większości przypadków wymaga autoryzacji użytkownika. Niestety, większość istniejących technik uwierzytelniania tworzy dość słabe powiązanie z rzeczywistą tożsamością użytkownika, a inne, takie jak dokumenty tożsamości, są bezużyteczne w przypadku transakcji elektronicznych gdyż są niczym więcej niż kawałkiem papieru lub plastiku, bez faktycznego połączenia z systemem elektronicznym. Jednocześnie, bezpieczny podpis elektroniczny oparty o tradycyjne PKI polega na zaufaniu przekazywanemu poprzez komercyjne podmioty, za pomocą certyfikatów. Proponowany protokół weryfikacji tożsamości łączy funkcjonalność narodowego elektronicznego dokumentu tożsamości z bezcertyfikatową kryptografią klucza publicznego (CL-PKC) aby zapewnić bezpieczny i godny zaufania sposób weryfikacji tożsamości, łączący większość zalet aktualnych rozwiązań i ograniczający wady do minimum.

Słowa kluczowe: weryfikacja tożsamości, uwierzytelnianie, bezpieczeństwo informacji.

1. Problem of identity verification and cryptography

Identity verification is a common problem, present in almost every kind of information system, relying on the very same scheme:

- E-banking (money transfers, opening/closing deposits, ordering services)
- E-voting (verification of eligibility for voting)
- E-commerce (confirmation of order request, provision of personal details)
- E-PUAP (verification of source of request for chosen governmental information)
- E-medicine (access to medical data, remote diagnosis or treatment, prescriptions)
- E-drugstore (buying out prescriptions over the Web)
- Car security (e-ID as a key)

There are dozens of documents proving identity – those pieces of paper or plastic become insufficient in the times of widespread e-everything, so some of them are being replaced by their electronic counterparts (for example Poland is working under a project called PL-ID, which stands for electronic personal identity document [1]), but their development is limited by the law meant to protect personal details of people and prevent identity theft). Only selected information can be available in this way [2] and, according to the law about securing personal identity data, each usage of such information must be accepted by their owner [3]. Fig. 1 presents identified universal process of identity verification in electronic environment with e-ID documents owned by all sides.

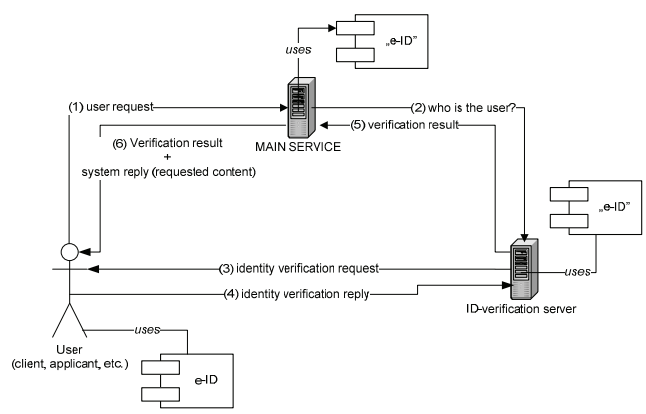

Fig. 1. Schematic idea of the proposed authentication protocol
Rys. 1. Schemat idei proponowanego protokołu uwierzytelniania

The most widely spread basis for digital signature is Public Key Infrastructure (PKI), which includes definitions of all mathematical operations, and their sequence, to perform proper digital signature [4]. Unfortunately, primarily there was too weak binding between the signature and the identity, as RSA (the basic algorithm for keys generation) does not require any personal details in key generation process [5]. To avoid frauds, certificates were designed as a source of authenticity proof for a digital signature. Certificate verification, however, requires performing

calculations that are especially costly in mobile environment [6]. Many other problems with traditional PKI were a subject of multiple articles, e.g. [7].

CL-PKC was proposed as a solution of PKI problems. It is a public key cryptography variation based on elliptic curves - a result of earlier research under utilization of bilinear pairings in cryptography, summarized in [8], where pair of keys is generated partially by Key Generation Center (a kind of Trusted Third Party in traditional PKI), and partially by the owner of keys himself. CL-PKC was introduced by Sattam S. Al-Riyami and Kenneth G. Paterson in [9].

The proposed solution joins security of traditional PKI based solutions, relying on utilization of a digital signature with the qualified certificate, with much simpler infrastructure offered by certificateless cryptography and electronic documents proving real identity. Such combination, however not yet in common use, solves most problems with authentication of previously unknown individuals on service access request.

Section 2 presents the proposed protocol. It contains a description of exchanged messages and the idea behind the protocol itself.

Section 3 discusses the results of the protocol verification according to BAN logic. Both assumptions and results of the protocol are shown and explained.

2. The proposed authentication protocol

The authentication protocol is believed to be good if sent authentication information contains features of undeniable proof. This definition does not require authenticated sides to communicate directly with each other. Usually communication is done with the help of dedicated authentication sides. According to G.Lowe in [10] the following definition of authentication can be used:

We say that a protocol correctly achieves authentication if whenever an agent A accepts the identity of another agent B, it must be the case then B believes that he has been running the protocol with A, and the records of the messages sent and received at the two ends should match (and similarly when B accepts A's identity). That is, if B sent a message m intended for A, then A received a message m apparently from B, and vice versa. We further require that there is a one-one relationship between A's runs and those of B, so A does not believe he has completed two runs, when B has carried out only a single run, for example.

The definition above says that once the protocol is finished both sides taking part in it agree to the information state in which partner ended, once the other side finished the protocol. The same should be true also when more than two sides take part in the protocol.

The goal of the proposed authentication protocol (see Fig. 1) is to confirm (or deny) the claimed identity of Side A and authorization of the requested operation by Side A. This means that the proposed protocol is meant to verify identity of Side A and confirm that Side A was the one who requested operation that triggered the whole process. At the same time, binding between the person's identity and requested operations should be protected from being hijacked or other third party misuse.

The proposed protocol uses CL-PKC to generate keys, sign, encrypt and decrypt messages, exactly as Sattam S. Al-Riyami and Kenneth G. Paterson described it in [9].

Actors included in the protocol:
- Side A (a person or a company)
- ID verification System (Side B)
- Main service (Side C) – holder of the content requested by Side A

The proposed protocol includes the following elements:
- z_1 – request message of Side A; must include random value
- a – random value | time stamp (session ID between B and C)
- $b = (b_1|b_2)$ – challenge value (b_1, b_2 – random numbers)
- $b' = (b_2+n|b_1)$; response value; n – second of current day
- IDT_A – temporary (random) identifier of side A
- KE_n = <XEn, YEn> – public key of Side n (encryption)
- KE_{n-1} – private key of Side n (decryption)
- KS_n = <XS_n, YS_n> – public key of Side n (verification of signature)
- KS_{n-1} – private key of Side n (signature generation)
- $(M)KE_n$ = <U, V, W> – message M encrypted with a public key KE_n by Side n
- id_{KGC} – KGC (Key Generation Center) identifier
- ID_n – identity data of Side n
- $Sig_n(M)$ = <U, v> - message or document M signed by Side n with the use of private key KS_{n-1}
- $H(x)$ – hash value of x (eg. SHA-512, see [11])
- f – result of identity verification (if positive – $H(ID_A)$; if negative – error number)
- z_2 – answer of main system, includes result of identity verification result of requested operation

The protocol relies on exchange of six messages:

1) $A \rightarrow C: z_1$

2) $C \rightarrow B : \left(Sig_C\left(H\left(z_1\right), IDT_A, a\right)\right)KE_B$

3) $B \rightarrow A : Sig_B\left(KS_B, ID_B, H\left(a\right), b, H\left(z_1\right)\right)$

4) $A \rightarrow B : Sig_A\left(H\left(ID_A\right), id_{KGC}, KE_A, KS_A, H\left(a\right), b', H\left(z_1\right)\right)$

5) $B \rightarrow C : \left(Sig_B\left(f, H\left(z_1\right), IDT_A, KE_A\right)\right)KE_C$

6) $C \rightarrow A : \left(Sig_C\left(z_2, H\left(a\right), H\left(z_1\right)\right)\right)KE_A$

The protocol, in fact, consists of two sessions. The first one is started by the main service (Side C) and covers communication between Main Service and ID verification system (Side B). The other session is between Side B and the User (Side A) and is started by Side B at the moment of identity claim request. Introduction of two session tokens (a, $H(a)$) increases security of the whole procedure by separating freshness marker of communication with Side A from the one of communication with Side C. It is assumed that Main Service is capable of securing its own sessions, once started, between Side A and Main System (Side C).

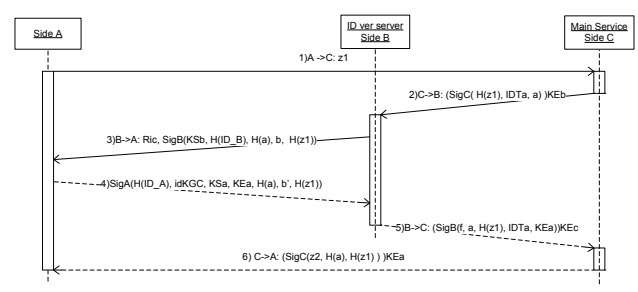

Fig. 2. The proposed ID verification protocol – sequence diagram
Rys. 2. Proponowany protokół weryfikacji tożsamości – diagram sekwencji

Fig. 2 presents the protocol. To start verification, both sides must hold a valid e-ID document, with properly generated pair of keys, meant for message encryption and a pair of keys for certificateless signature. Although KGC is not present here, it may be referenced at the moment of verification of public keys or signatures – to obtain params and KGC's public keys. This, however, is optional as both keys and params can be stored locally by Side B and updated periodically.

3. Verification of the proposed protocol

To prove security of the protocol, BAN logic was used to verify each message. This type of logic was proposed by Burrows, Abadi and Needham and described in [12]. It relies on following symbols:

$P \mid\equiv X$: P believes in X, P can be sure that message X is true.

$P \lhd X$: P can see X which means, that someone sent a message containing X to P; P may read X and try replying to message X.

$P \mid\sim X$: P once said (sent) X (P sent message containing X); it cannot be said whether the message belongs to current session or not, but it is true that P trusted message X when it was sent.

$P \Rightarrow X$: P can confirm that X is true; this construction is used to delegate permissions.

$\#(X)$: message X comes from current protocol session (is fresh).

$P \xleftrightarrow{K} Q$: sides P and Q use shared symmetric key K.

$\xrightarrow{K} P$: side P owns public key K; private key is well protected.

$\{X\}_K$: operation with a use of cryptographic key K is done on message X (it can be symmetric key, public key or private key).

According to the basic rules of BAN, the proposed protocol is converted to an idealized form first:

- Message 1:

plain text message – has no influence.

- Message 2:

$$C \rightarrow B : \left\{\left\{IDT_A, a, H(z_1)\right\}_{KS_C^{-1}}\right\}_{KE_B}$$

- Message 3:

$$B \rightarrow A : \left\{\xrightarrow{KS_B} B, ID_B, H(a), b, H(z_1)\right\}_{KS_B^{-1}}$$

- Message 4:

$$A \rightarrow B : \left\{H(ID_A), id_{KGC}, \xrightarrow{KS_A} A, \xrightarrow{KE_A} A, H(a), b', H(z_1)\right\}_{KS_A^{-1}}$$

- Message 5:

$$B \rightarrow C : \left\{\left\{f, a, IDT_A, \xrightarrow{KE_A} A, H(z_1)\right\}_{KS_B^{-1}}\right\}_{KE_C}$$

- Message 6:

$$C \rightarrow A : \left\{\left\{z_2, H(a)\right\}_{KS_C^{-1}}, H(z_1)\right\}_{KE_A}$$

It is assumed that keys KE_B, KE_C, KS_B, KS_C were exchanged earlier with the help of a separate procedure that guarantees their source and validity and, as a result, binding between the key and identity is trusted.

The detailed analysis starts from message 2. According to BAN logic, meaning of the message, its freshness and jurisdiction was verified. The result of such analysis and analysis of Message 5 and Message 6 allow coming with the following results, where the results from Message 2 create further Assumption for analysis of Message 3 and Message 4.

The following assumptions must be made:

- $C \mid\equiv \xrightarrow{KE_B} B, B \mid\equiv \xrightarrow{KE_C} C,$
  $C \mid\equiv \xrightarrow{KS_B} B, B \mid\equiv \xrightarrow{KS_C} C$
- $C \mid\equiv \#(a), C \mid\equiv \#(IDT_A), A \mid\equiv \#H(z_1), A \mid\equiv \#(b'), B \mid\equiv \#(b)$
- $B \mid\equiv C \Rightarrow (IDT_A, a), A \mid\equiv B \Rightarrow \left(\xrightarrow{KS_B} B, ID_B, b\right)$
- $B \mid\equiv A \Rightarrow \{H(ID_A), \xrightarrow{KS_A} A, \xrightarrow{KE_A} A, b', H(z_1)\}$

The results of the protocol are:

- $B \mid\equiv H(ID_A)$ from eq. (10) and $A \mid\equiv H(ID_B)$ form eq. (5)
- $C \mid\equiv B \mid\equiv H(ID_A)$, $C \mid\equiv H(ID_A)$ from analysis of Message 5
- $C \mid\equiv f, C \mid\equiv z_1$ from analysis of Message 5
- $A \mid\equiv z_2$ from analysis of Message 6

In Fig. 1 it can be seen that the core of the authentication process is done between Side A (the user) and Side B (the ID verification server). Side C (Main service) is only a passive observer of this part of the authentication protocol, interested in its final result only. Because of that, only the analysis of Message 3 and Message 4 is presented below, while the analysis of Message 2, Message 5 and Message 6 is shortly described.

The analysis of Message 2 shows that Side B believes that main service once sent (said) the temporary identifier of A, the session token a and hash of Side A request. Freshness of this message can be verified on the basis of time stamp value added to session token a, so it has accuracy equal to the acceptable latency.

Message 3:

Meaning:

$$\frac{A \mid\equiv \xrightarrow{KS_B} B, A \lhd \{\xrightarrow{KS_B} B, ID_B, H(a), b, H(z_1)\}_{KS_B^{-1}}}{A \mid\equiv B \mid\sim \{\xrightarrow{KS_B} B, ID_B, H(a), b, H(z_1)\}} \quad (1)$$

Freshness:

$$\frac{A \mid\equiv \#(H(z_1))}{A \mid\equiv \#\left(\xrightarrow{KS_B} B, ID_B, H(a), b, H(z_1)\right)} \quad (2)$$

$$\frac{A \mid\equiv \#\left(\xrightarrow{KS_B} B, ID_B, H(a), b, H(z_1)\right), A \mid\equiv B \mid\sim \{\xrightarrow{KS_B} B, ID_B, H(a), b, H(z_1)\}}{A \mid\equiv B \mid\equiv \{\xrightarrow{KS_B} B, ID_B, H(a), b, H(z_1)\}} \quad (3)$$

$$\frac{A \mid\equiv B \mid\equiv \{\xrightarrow{KS_B} B, ID_B, H(a), b, H(z_1)\}}{A \mid\equiv B \mid\equiv \{\xrightarrow{KS_B} B, ID_B, b\}} \quad (4)$$

Jurisdiction:

$$\frac{A \mid\equiv B \Rightarrow \left(\xrightarrow{KS_B} B, ID_B, b\right), A \mid\equiv B \mid\equiv \{\xrightarrow{KS_B} B, ID_B, b\}}{A \mid\equiv \{\xrightarrow{KS_B} B, ID_B, b\}} \quad (5)$$

Message 4:

Meaning:

$$\frac{B \mid\equiv \xrightarrow{KS_A} A, B \lhd \{H(ID_A), id_{KGC}, \xrightarrow{KS_A} A, \xrightarrow{KE_A}, H(a), b', H(z_1)\}_{KS_A^{-1}}}{B \mid\equiv A \mid\sim \{H(ID_A), id_{KGC}, \xrightarrow{KS_A} A, \xrightarrow{KE_A}, H(a), b', H(z_1)\}} \quad (5)$$

Freshness:

$$\frac{B \mid\equiv \#(b)}{B \mid\equiv \#(b')} \quad (6)$$

$$\frac{B \mid\equiv \#(b')}{B \mid\equiv \#\left(H(ID_A), id_{KGC}, \xrightarrow{KS_A} A, \xrightarrow{KE_A} A, H(a), b', H(z_1)\right)} \quad (7)$$

$$\frac{B \mid\equiv \#\left(H(ID_A), id_{KGC}, \xrightarrow{KS_A} A, \xrightarrow{KE_A} A, H(a), b', H(z_1)\right), B \mid\equiv A \mid\sim \{H(ID_A), id_{KGC}, \xrightarrow{KS_A} A, \xrightarrow{KE_A} A, H(a), b', H(z_1)\}}{B \mid\equiv A \mid\equiv \{H(ID_A), id_{KGC}, \xrightarrow{KS_A} A, \xrightarrow{KE_A} A, H(a), b', H(z_1)\}} \quad (8)$$

Jurisdiction:

$$\frac{B \mid\equiv A \Rightarrow \{H(ID_A), \xrightarrow{KS_A} A, \xrightarrow{KE_A} A, b', H(z_1)\}, B \mid\equiv A \mid\equiv \{H(ID_A), \xrightarrow{KS_A} A, \xrightarrow{KE_A} A, b', H(z_1)\}}{B \mid\equiv \{H(ID_A), \xrightarrow{KS_A} A, \xrightarrow{KE_A} A, b', H(z_1)\}} \quad (9)$$

$$\frac{B \mid\equiv \{H(ID_A), \xrightarrow{KS_A} A, \xrightarrow{KE_A} A, b', H(z_1)\}}{B \mid\equiv \{H(ID_A)\}} \quad (10)$$

In case of Message 5, Side C believes that Side B once sent that message and thanks to the fact that it is able to verify freshness of the session token a, it can be said that Side C believes that Side B believes in the content of that message. As this message contains the result of identity verification, which (if positive) includes hash of Side A identity, it can be said that Side C believes that Side B believes in that identity. Because Side C has jurisdiction over the whole Message 5 content, it can finally be said that Side C believes in the provided identity.

Similarly, in Message 6 Side A can verify freshness of hash of its own request, so it is able to prove both meaning and freshness of the whole message received. As a result, Side A believes that Side C believes in the content of that message. On that basis, with the help of the fact that Side C has jurisdiction over most of Message 6 content (including z_2), it can be said that Side A believes in z_2.

As can be seen, B gains trust to the claimed personality. That trust is then transferred to Main Service. The source of trust, from point of view of side C, concentrates on freshness of session token and a temporary identity of side A (which were earlier generated by side C) and verification of side B signature. Similarly, Side A gained trust to the identity of Side B, which is the verification system. This means that the client of main service knows who is responsible for verification of his identity and, as a result, who will receive and process hashes of his identity details. Trust on this level means also that, because Side A knows whom it is talking to, it will be able to detect and prove attempts of frauds based on fake identity verification service joining in the middle of the protocol e.g. to transfer the client to a fake main service. As a result, the received data may be rejected if Side A cannot trust that what was received is a result of identity verification performed by Side B.

From the main service point of view, to trust identity of Side A, it must gain trust to the results of identity verification and to identity of Side B as well. Trust to identity of Side B is gained earlier, prior to the proposed protocol, at the moment of exchange of public keys. That trust is then verified passively (message 2 is encrypted, which allows assumption that only a holder of the proper private key, which is believed and trusted to be Side B can decrypt the message) and actively (message 5 is signed by Side B, which allows verification of the source of the message with the help of keys exchanged earlier). Moreover, Side C receives confirmation of Side A request content (shown as z_1). This means that the client confirmed his expectations and that it can be assumed that nothing was changed since message 1 was generated (e.g. by some other party).

Finally, Side A, which is the client of main service, gains trust to the results of verification and the data received from Side C. That trust comes basically from trust to the identity of Side B, which has already been described. That trust is strengthened by verification of Side C signature under the received data. This creates a strong binding between the main service and identity verification system that was used in the current session, which is fully verifiable.

4. Results and conclusions

To prevent information leaks and various types of frauds, many methods of identity verification were developed. Their most common problem, however, is very weak binding with real identity. The biggest advantage of the proposed solution is strong binding with the real identity and the source of trust, which relies fully on a government institution and document it issues. What is more, lack of certificates simplifies the system structure and decreases the number of additional services required. As keys are bound with identity on the level of generation, there is no need to add separate elements to bind keys with identity.

5. References

[1] plID: http://www.cpi.mswia.gov.pl/portal/cpi/38/178/plID.html

[2] Act on population registry and identity cards (in polish), from April 10th, 1974 – an uniform text (Law Diary - Dz.U. no 87/2001, pos. 960, with later amendments).

[3] Act on personal data protection (in polish), from August, 29th, 1997 (Law Diary - Dz. U. 1997 no 133 pos. 833, with later amendments).

[4] Barr D.: Public Key Infrastructure, Technology and Programs Division, Technical Notes, Vol. 11, Number 3, December 2004.

[5] Rivest R.L.: A. Shamir, L.M. Adleman, A Method for Obtaining Digital Signatures and Public-key Cryptosystems, Communications of the ACM 21 2 (Feb. 1978), 120-126, 1978.

[6] Dankers J.: T. Garefalakis, R. Schaffelhofer, T. Wright, Public Key Infrastructure in mobile systems, IEE Electronics and Communications Engineering Journal, 14(5) :180-190, 2002.

[7] GutmannP.: PKI: It's not dead, just resting., IEEE Computer, 35(8):41;49, 2002.

[8] Patterson K.: Cryptography from pairings: a snapshot of current research, Information Security Technical Report, Vol. 17, No. 3, 2002.

[9] Al-Riyami S., Paterson K.: Certificateless Public Key Crypto-graphy, AsiaCrypt proceedings, 2003.

[10] Lowe G.: Some new attacks upon security protocols, Proceedings of the 9th IEEE workshop on Computer Security Foundations, IEEE Computer Society Washington, DC, USA, pp.162-169, 1996.

[11] Secure Hash Standard, Federal Information, Processing Standards Publication 180-2, NIST, 2002.

[12] Burrows M., Abadi M., Needham R.: A Logic of Authentication, SRC Research Report 39, Digital Equipment Corporation, 1990.

otrzymano / received: 21.09.2010
przyjęto do druku / accepted: 01.11.2010 *artykuł recenzowany*