



CRYPTOMATHIC

Den Gode Webservice - Security Analysis

**Cryptomathic A/S
September, 2006**

Executive Summary

This report analyses the security mechanisms provided in Den Gode Web Service (DGWS). DGWS provides a framework securing messages at 5 different security levels based on IDCards with authentication level 1, 2, 3 or 4. Security level 1 only provides identification, level 2-4 provides some level of authentication (i.e., proof of identity) and level 5 provides message authentication.

Security levels 1, 2, 3 and 4 add very little security as the mechanisms at this level are vulnerable to replay attacks and these mechanisms depend completely on the confidentiality and integrity provided by the network. The main recommendation is therefore to concentrate DGWS on transactions at security level 5 and develop profiles for different usages of digital signatures. Depending on whether MOCES or VOCES certificates are used, it is possible to define different security levels depending on whether the service requires message authentication or non-repudiation.

It is further suggested that DGWS clarifies the risk of using a revoked certificate when relying on IDCards signed by the Identity Provider. The consequences of this depend on the sensitivity of the service and must be well understood.

Table of Contents

Executive Summary	2
References	4
1 Introduction	5
1.1 Purpose	5
1.2 Scope	5
1.3 Target	5
1.4 Document Organisation	5
2 Terminology	6
3 Overview of DGWS	7
3.1 Entities and Services.....	7
3.2 IDCard	7
3.3 Envelopes.....	9
3.4 Security Levels	9
4 Analysis	10
4.1 Cryptographic Issues.....	10
4.2 Certificate Management	10
4.3 Identification and Authentication	11
4.4 Message Authentication	12
4.5 Single Sign-On	13
4.6 Request-Response and Sessions.....	13
4.7 Confidentiality.....	14
4.8 Integrity.....	14
5 Conclusion and Recommendations	15



References

- [CPMOCES] *Certifikatpolitik for OCES-medarbejdercertifikater (Offentlige Certifikater til Elektronisk Service)*. Version 4.0, August 2005. See <https://www.signatursekretariatet.dk/certifikatpolitikker.html>
- [CPVOCES] *Certifikatpolitik for OCES-virksomhedscertifikater (Offentlige Certifikater til Elektronisk Service)*. Version 3.0, August 2005. See <https://www.signatursekretariatet.dk/certifikatpolitikker.html>
- [DGWS] *Den Gode Webservice*, MedCom. Version 1.0, July 13, 2006.
- [DGWSB] *Den Gode Webservice - Bilag*, MedCom. Version 1.0, July 13, 2006.



1 Introduction

1.1 Purpose

The purpose of this document is to analyse the security offered by Den Gode Webservice (DGWS) as described in [DGWS]. This includes describing the features and limitations of the security mechanisms within DGWS and identifying prerequisites for exploiting these.

1.2 Scope

DGWS defines a web service profile specifying how a number of standards must be used for web services within the Danish Health Care. As part of this, mechanisms for identification and authentication of the sender of a message are defined. This document analyses these security mechanisms and identifies possible security problems when basing transactions on DGWS. Prerequisites for utilising these mechanisms are identified and a few recommendations are given.

Only the profile defined in [DGWS] is considered. This document does not deal with actually implemented services based on the profile.

DGWS is based on a number of standards including standards for secure web services. This document neither analyses these standards nor the actual use of them. Only the resulting security mechanisms are considered.

In order to establish a secure system, the platforms running the components must be secured. This includes (but is not limited to) proper network configuration and protection against malware. It is out of the scope to consider methods for securing the platform.

1.3 Target

This document targets readers interested in the security properties of DGWS either as part of implementing systems/services based on DGWS or as part of evaluating the security of actual services based on DGWS.

1.4 Document Organisation

It is assumed that the reader knows DGWS, but in order to make the document self-contained, the central (security) mechanisms used by DGWS are briefly reviewed in section 3. The actual analysis is presented in section 4 and conclusions as well as recommendations are given in section 5.

2 Terminology

Authentication	Ensuring that an entity has the claimed identity.
Availability	Reliability and accessibility of data and resources
Confidentiality	Protecting the data from being disclosed to unauthorised parties.
Identification	Identifying an entity.
Integrity	Ensuring that data are not changed by unauthorised entities.
Message Authentication	Ensuring that a message originates from a particular user. Implies integrity.
MOCES certificate	Danish “Medarbejder OCES” certificate
MOCES signature	Digital signature created with private key corresponding to MOCES certificate.
VOCES certificate	Danish “Virksomheds OCES” certificate (certificate belonging to company – typically used by several systems within the company).
VOCES signature	Digital signature created with private key corresponding to VOCES certificate.



3 Overview of DGWS

A comprehensive description of DGWS can be found in [DGWS, DGWSB]. Briefly, the goal of DGWS is to provide a profile for securing Web services.

While information security generally deals with availability, confidentiality and integrity, the purpose of DGWS is to support mechanisms for identification, authentication and message authentication. Confidentiality and availability are not within the scope of DGWS. Furthermore, for mechanisms providing identification and authentication, integrity must be ensured by different means.

In order to obtain confidentiality and integrity, [DGWS] recommends running DGWS over networks using either VPN (as in the closed health care network) or SSL. Availability is not addressed in [DGWS] and, although essential, will not be discussed further here.

The overview below describes how DGWS provides identification and (message) authentication.

3.1 Entities and Services

DGWS covers the following entities:

- A number of clients.
- A number of service providers.
- An Identity Provider (IdP), which is a special service provider issuing IDCards (see section 3.2).

A Web service consists of one or more pairs of (request, response). The following three types of services are supported in DGWS:

Inquiry	Client requests data from service provider.
Message	Client provides information to service provider (the response is a receipt).
Session	A number of inquiries and messages linked together.

3.2 IDCard

All requests and certain responses contain an IDCard. An IDCard contains the following information:

- Validity period (typically 24 hours).
- Card information (including information about issuer of card).
- User Information – identifies the owner of the IDCard.
- System Information.



- Security credentials.

The detailed content depends on the authentication level (1, 2, 3 or 4) and is described in [DGWSB]. For this analysis, it is important to understand the security related information (in particular security credentials) within the card. At level 3 and 4, either the client or the IdP signs the card:

Authentication level	Security information
1	None.
2	Username and password
3 (ID card signed by user)	Card Information contains hash of client VOCES certificate. Security credentials contain <ul style="list-style-type: none"> • Clients VOCES certificate • Signature on IDCard using private key corresponding to client VOCES certificate
3 (ID card signed by IdP)	Card Information contains hash of client VOCES certificate. Security credentials contain <ul style="list-style-type: none"> • IdP VOCES certificate^{*)} • Signature on IDCard using private key corresponding to IdP VOCES certificate
4 (ID card signed by user)	Card Information contains hash of client MOCES certificate. Security credentials contain <ul style="list-style-type: none"> • Clients MOCES certificate • Signature on IDCard using private key corresponding to client MOCES certificate
4 (ID card signed by IdP)	Card Information contains hash of client MOCES certificate. Security credentials contain <ul style="list-style-type: none"> • IdP VOCES certificate^{*)} • Signature on IDCard using private key corresponding to IdP VOCES certificate

^{*)} When IdP signs the card, it either includes its certificate or a reference to its certificate.

As part of issuing an IDCard, the IdP verifies that the client certificate is not revoked. A service provider trusting IdP can therefore assume that the client certificate was valid at the time the IDCard was *issued* and may therefore opt not to validate the client certificate itself, thereby avoiding the trouble of checking revocation.

3.3 Envelopes

Requests and responses are transmitted in SOAP envelopes. Such an envelope contains a header and a body. The actual payload of the request/response is in the body. The IDCard is inserted in the header.

If the IDCard has authentication level 3 or 4, the header may, in addition, contain a signature on the entire envelope (i.e. including the IDCard). This signature also contains the client certificate and is validated in the following three steps (in addition to validation of certificate status):

1. Validate IDCard (against known IdP certificate or client certificate within IDCard).
2. Validate signature on envelope against client certificate included in signature.
3. Validate client certificate in envelope signature against hash value of client certificate within IDCard information.

[DGWS] and [DGWSB] focus on the use of IDCards in relation to requests from clients. However, it is understood that IDCards and signed envelopes can also be applied to responses from the service provider to a client, if necessary.

3.4 Security Levels

DGWS defines the security of a particular web service by two parameters: security level (1, 2, 3, 4 or 5) and time-out (levels 1, 2, 3 or 4).

Security levels 1, 2, 3 and 4 are equivalent to using cards with the corresponding authentication level as defined above. Security level 5 is equivalent to using a level 3 or 4 card with a digital signature on the envelope as described in section 3.3.

Time-out levels define how long the service provider will accept the IDCard after it has been issued (24 hours, 8 hours, 30 minutes or 5 minutes).



4 Analysis

The analysis is structured in a bottom up fashion first considering the cryptographic primitives and certificate handling, then the security mechanisms supported by DGWS and finally some thoughts on the overall security.

In the analysis below, the term “relying party” denotes the entity validating an IDCard or, for security level 5, a signature on an envelope. In most cases, the relying party will be a service provider, but it could also be the client system.

4.1 Cryptographic Issues

DGWS uses RSA and SHA-1. The choice of RSA for signing is enforced by OCES and is in line with current practice.

In recent years, the security of SHA-1 has been questioned by improved cryptographic attacks. Although there is no reason to immediately stop using SHA-1, it is recommended that DGWS be prepared for using other hash functions.¹ While it may be difficult for DGWS to unilaterally replace SHA-1 in digital signatures as the OCES certificates are used with different applications, it could be considered to use SHA-256 when computing the hash value of the client certificate in level 3 and 4 cards.

The security of IDCards of authentication level 3 and 4 depends crucially on the security of the private keys used to sign them. These keys must therefore be managed very securely in clients and service providers. Private keys corresponding to VOCES certificates may be used by several systems and activated by several users within a company or institution. Procedures controlling access to these keys (including password control) must therefore be carefully implemented at client systems as well as service providers.

Special attention must be paid to the private key of IdP, since a number of service providers are expected to rely on the IDCards it issues. Access to this key can be better controlled by placing the IdP system in a secure rooms and/or having the private key in secure cryptographic hardware security modules.

4.2 Certificate Management

Relying parties validating IDCards and signed messages must have installed the TDC OCES CA root certificate and ensure that the signature is validated against it. If the relying party has installed other trusted certificates, it must be ensured that the certificate is validated against the TDC OCES CA certificate. If the relying party is a client using a browser based application, special care should be taken to prevent validation against other CA certificates, which are installed as trusted in the browser. Otherwise a door for accepting fake certificates may be opened.

¹ There are activities towards recommending a replacement for SHA-1. While these are still in progress, the currently best candidate is SHA-256.

It is assumed in this analysis that when IdP issues an IDCard, it has properly validated the client certificate against the TDC root and against the latest revocation information from TDC². This may reduce the burden of the service provider, but introduces the risk that the certificate has been revoked after the IdP issued the IDCard, but before the card is used. If the relying party does not validate the certificate status, the period for using a revoked certificate is increased from 1 minute and up to the service time-out period. This risk must be weighed against the computational and administrative advantages for each service provider taking the sensitivity of the service into account.

An IDCard issued by IdP refers to IdP's certificate using a serial number. The specification is not clear here:

- In [DGWS, p16] the subject serial number (cvt-rid value) is suggested to be used. However, this value is not likely to be changed when the certificate is renewed. Using this value therefore enables a situation where an IDCard can be validated against the wrong (expired) key.
- In [DGWSB, p52] the certificate serial number is suggested. This serial number is unique for a particular CA and therefore provides a better reference. However, certificates issued by other CAs may potentially have the same serial number. Therefore the relying party must, as discussed above, ensure that IdP's certificate is issued by TDC OCES CA.

In general, procedures must be established for installing IdP's certificate correctly at all relying parties. This includes validating that the correct certificate is installed, effecting procedures for updating it and continuous validating that it is not changed (e.g. by malware). Procedures for handling revoked IdP certificate must be in place at all relying parties.

4.3 Identification and Authentication

The following considers messages on security level 1, 2, 3 and 4.

An IDCard identifies a certain party in the system. The IDCard is neither linked to a particular relying party (e.g., a service provider) nor to a particular message. This means that the same IDCard can be used in a number of different transactions.

IDCards at authentication level 1 are not secured (except for the security offered by the network) and are only used to convey identification.

For authentication level 2, the IDCard can only be used with relying parties for which the username and password are registered. It does not appear clearly from [DGWS] if the same username/password can be used with more than one service provider, but DGWS does not restrict the IDCard to a single provider. If a malicious party gets a level 2 card, it also gets the corresponding username/password, and can therefore construct such cards

² When a certificate is revoked, TDC must provide an updated CRL within one minute (see [CPMOCES, CPVOCES])

by itself at any time. Thus the confidentiality provided by the system (including, but not limited to, the network) is essential for the reliability of authentication at this level.

For cards with authentication level 3 and 4, the IDCard can be used with all service providers accepting the corresponding security level. In particular, if a malicious party gets the IDCard of another entity, that malicious party can use the IDCard in the same transactions as the rightful owner (masquerading) during the given validity period and limited by the service time-out. Forging or changing existing IDCards of level 3 or 4 requires a digital signature. If the owner's private key is not compromised, this can be assumed infeasible. Therefore, the malicious party can only use the eavesdropped IDCard during its validity period (again limited by the time-out policy of the service provider).

[DGWS, p. 22] mentions that some service providers require that the user enter a new password at every message. This is enforced by having a 5-minute time-out. However, as mentioned above the same IDCard may potentially be used with different service providers and therefore this requirement is not strictly enforced by a 5-minute time-out. Furthermore, even if the card can only be used with one service provider (possible at authentication level 2), several transactions can be made within 5 minutes using the same card. This can be remedied using the following mechanisms for level 3 and 4 cards:

- IDCard (preferably the entire transaction) is made dependent on service provider; and
- service provider ensures that a particular card is only accepted once.

4.4 Message Authentication

Message authentication is only supported at security level 5, where cards with authentication level 3 and 4 are used with enveloped signing. The receiving entity will in all other situations (i.e., security level 1-4) have no guarantee about the integrity and origin of the message except what is provided by the underlying network.

If level 3 cards are used in combination with envelope signing, the recipient is guaranteed that the message originates from a system having access to the private key. By the properties of VOCES certificates, this does not guarantee that the message originates from a particular user. An audit log within the originating system should be maintained in order to identify the originator.

If level 4 cards are used in combination with envelope signing, the recipient is guaranteed that the message originates from the person identified in the MOCES certificate (assuming the key is not compromised).

In [DGWS], security level 5 is called "non-repudiation". It is worth recalling the difference between VOCES and MOCES signatures and remembering that non-repudiation requires more than just a digital signature (such as procedures and mechanisms for storage, retrieval and independent signature validation). For this reason, the term "message authentication" is applied here, and it is noted that MOCES signatures can be used as a first step towards non-repudiation.

It may be considered to combine IDCards at level 4 with VOCES signatures on the transaction in cases where message authentication, but not non-repudiation is required: While the card ensures that the user has been logged on (when making the card), the VOCES signature provides message authentication. The value of this combination depends on the actual services. It can be included in the current profile by extending IDCards to contain both MOCES and VOCES certificates.

Finally, it is noted that even if a malicious party obtains another entity's IDCard, that party cannot sign the envelope. Therefore security level 5 enables strong linking of request and responses (see also section 4.6 regarding linking) as well as strong linking of transactions to clients and service providers preventing a number of replay attacks. However, to fully benefit from this, DGWS must define a profile for signed messages defining required attributes.

4.5 Single Sign-On

The security properties of level 3 and 4 IDCards are independent of whether the IdP or the owner signs the card, except that relying parties, as discussed in section 4.2, may save some certificate validation when the IdP has signed the card.

It is worth noting, however, that a malicious party observing the request for an IDCard at the IdP may replay this request in order to get another IDCard (for the original entity) signed by IdP. In transactions with security level 3 and 4, this card can be (mis)used in the same way as a copied card (see section 4.3). This card will be slightly different from the one obtained by the owner and can therefore be used in transactions of level 3 and 4, even if the service provider tries to avoid accepting the same card twice.

The IdP must prevent this by storing requests of IDCards until the card in the request expires.

[DGWS] does not specify the validity period of an IDCard issued by IdP. If it is valid for 24 hours after the IdP *signs* the card, an eavesdropped card signed by the owner can in principle be used for up to 48 hours. Namely, first the eavesdropped card is used for almost 24 hours and then, just before it expires, the attacker uses it in a request for a new card at the IdP. This card issued by the IdP can then be used for up to 24 hours.

4.6 Request-Response and Sessions

Messages are made unique by inserting a unique message ID in each message. A recipient can therefore in principle detect replay by storing all received message IDs (as long as the message is valid). This mechanism does not, however, prevent a malicious party from replaying a message with a new message ID. Even if the network provides adequate integrity protection, the replayed message could be injected.

DGWS does not securely link the response to the request. Unless the underlying network security prevents it, an attacker can therefore insert an arbitrary answer. If the response is signed, a link to the request can be added in the body, and the signature will then prevent replays of responses (see discussion in section 4.4).

All messages in a session (except the first request) contain FlowID, which is unique for that session. This allows both client and service provider to link envelopes in the session. Obviously this linking is only guaranteed to the extent that integrity is provided (by the network and/or digital signatures).

4.7 Confidentiality

DGWS does not provide any mechanisms ensuring confidentiality. As discussed above IDCards with authentication level 1, 2, 3 and 4 can be re-used by malicious parties (except in transactions of security level 5). It is therefore essential that the underlying network provide confidentiality in order to ensure the confidentiality of IDCards as well payload data.

[DGWS] suggests using VPN or SSL. Analysis of these mechanisms is out of the scope of this document, but some care is required if SSL is used, as there are advanced attacks (e.g., related to Internet banking) on web based applications, in which a user can be lured to malicious Web servers and perform transactions here, even if SSL is applied. Such a malicious Web server could also be used to obtain e.g., level 2, 3 or 4 ID Cards from a client system.

4.8 Integrity

As discussed above, only DGWS transactions of security level 5 provide message authentication. Transactions on security level 1, 2, 3 and 4 do not provide any authentication of the transmitted data.

5 Conclusion and Recommendations

DGWS provides a framework securing messages in Web services. It is recommended to implement this in such a way that the cryptographic hash function (SHA-1) can easily be replaced. Furthermore, SHA-256 should be used where possible.

DGWS uses IDCards with authentication level 1, 2, 3 or 4. Security level 1 only provides identification, level 2-4 provides some level of authentication and level 5 provides message authentication.

As security levels 3, 4 and 5 rely on public-key technology, all entities must manage keys and certificates carefully. Although self-evident, this point is often ignored.

As the IdP is a trusted party, special attention must be paid to the private key of the IdP and relying parties must manage the certificate of IdP very cautiously. It is recommended to base the implementation and policies of IdP on existing standards for trusted authorities.

For messages on security level 2-4, the authentication mechanism is only reliable to the extent that the underlying network provides confidentiality and integrity. However, independently of the network security, a receiving party (e.g., a malicious service provider) may reuse the IDCard (security level 2-4) in a masquerading attack. There are a number of examples of such malicious servers when SSL is the only network protection. A properly controlled, closed network (e.g., VPN) can be considered harder to infiltrate. The eavesdropped card can be used as follows:

- A malicious party can use an eavesdropped level 2 IDCard to create new valid IDCards for the original owner.
- A malicious party can use an eavesdropped level 3 or 4 IDCard in other transactions during the validity period of the IDCard. However, the malicious party cannot create new cards (as for level 2 cards), as this requires a digital signature.

IDCards at level 3 ensures that a particular system or company has participated in creating the cards. At level 4, it is ensured that a particular person has participated. In general, IDCards at security levels 2, 3 and 4 add very little security on their own as they are subject to replay attacks and these mechanisms depend completely on the confidentiality and integrity provided by the complete system (including service providers and network).

If the network does not provide sufficient integrity, level 3 and 4 cards can be used in combination with digital signatures to protect the authenticity and hence integrity of the messages.

In order to reduce the dependency on the security features of the network, it is, in any case, recommended to digitally sign transactions (i.e., level 5 is the preferred security level). Related to this, DGWS should be extended with a more detailed profile of signed envelopes (e.g., defining attributes for time stamps, recipient, linking of messages, ...).

If the message is signed corresponding to a VOCES certificate, it is ensured that the message originates from a particular system. But if the message is signed corresponding

to a MOCES certificate, it is ensured that the message originates from a particular user. It is suggested to consider the possibility of mixing level 4 IDCards with VOCES signatures on the transactions in the light of the required web services.

If the network cannot be trusted to provide confidentiality, it could be considered to integrate mechanisms for encrypting messages in DGWS. This is feasible as the required key material is available.

Finally, each service provider must carefully consider the level of trust to place in IDCards signed by IdP against the risk of accepting a revoked certificate. DGWS defines a time-out period for all services for managing this risk. However, the use of this parameter should be defined in more detail in relation to the sensitivity of the services. The use of a 5-minutes time-out to ensure that an IDCard is only used once is, at best, questionable. This goal is better achieved by using signed envelopes (security level 5) with strong links to the particular service.

