Security appendix

API-DEBT-FI

Version: 1.3.0

June 12th 2020

1 Introduction

This document is the security specification for Financial Institutions (FI) and debt portals/debt data registers (Debt Information Companies, DIC) to exchange information about debt. The security specification is defined by Norsk Gjeldsinformasjon AS, Gjeldsregisteret AS and Experian Gjeldsregister AS.

The security specification is created to ensure that the financial institutions does not need to adhere to multiple security standards. The objective is that all security aspects of delivery of debt information between financial institutions and Debt Information Companies shall be based on this standard.

This document will potentially be modified more frequently than the “Standard” document itself, based on threats and regulations in the security domain. Therefore, the document will constantly be source of revision, based on input from users and other professional environments/actors within security.

The document refers to several recommendations from well-known Norwegian security actors such as the Nasjonal Kommunikasjonsmyndighet (NKOM), the Nasjonal Sikkerhetsmyndighet (NSM) and the Direktoratet for forvaltning og ikt (Difi). These actors will also be a source for potential changes to this document.

1.1 Purpose of this document

The purpose of this document is to describe a standard to handle security aspects between financial institutions and Debt Information Companies. This document describes security mechanisms which will ensure integrity, confidentiality and availability for the interfaces provided by the financial institutions

The standard will only cover security related to the interface to provide debt information from the financial institutions to the Debt Information Company. Other security aspects related to the Debt Information Company is not in scope.

1.2 Audience

The audience for this document is Financial Institutions or Providers and Debt Information Companies.

1.3 Table of Contents

1 Introduction 2
1.1 Purpose of this document 2
1.2 Audience 2
1.3 Table of Contents 3
2 Information 4
2.1 Revision History 4
2.2 Reference Documents 4
2.3 Latest version of the document 4
2.4 Dictionary 5
3 Certificates 6
3.1 Enrollment – Creation and signing 6
3.2 Certificate Management 7
3.3 Use of certificates in communication between FI and DIC 8
4 HTTPS security details 10
4.1 Authentication of client and service 10
4.2 Authorization of client 10
4.3 Confidentiality 10
4.4 Data integrity 10
4.5 TLS transport requirements 10
5 Maintenance 11
6 Overall security requirements 12
7 Approved Qualified Trusted Service Providers 13

2 Information

2.1 Revision History

Version	Status	Date	Editor
V0.1	Draft	11.09.2018	EVRY/FNO
V0.2	Lagt inn felles endringer	19.09.2018	EVRY/FNO
V0.3	Etter verifikasjon og gjennomlesning	21.09.2018	EVRY/FNO
V0.4	Revidert etter tilbakemelding fra Buypass og Commfides	29.09.2018	EVRY/FNO
V0.5	Specification for client certificate, instructions for maintaining the document.	04.10.2018	EVRY/FNO
V0.6	Renewal and maintenance of both client and server certificates.	08.10.2018	EVRY/FNO
V1.0	The document validated by EVRY and FNO	10.10.2018	EVRY/FNO
V1.1	Fixed some typing errors	23.10.2018	EVRY
V1.2	Foreign FI's and service providers may use EV certificates from non-norwegian CAs	09.05.2019	Kantega
V1.3.0	Require EV server certificates, remove requirement for buying these from Buypass or Commfides. Allow eIDAS PSD2 – compatible client certificates from selected certificate authorities.	12.06.2020	Norsk Gjeldsinformasjon AS & Kantega

2.2 Reference Documents

Interface - Debt information from financial Gjeldsregisteret AS institutions

2.3 Latest version of the document

Latest version of this document may be obtained by contacting Norsk Gjeldsinformasjon AS, Experian Gjeldsregister AS or Gjeldsregisteret AS.

2.4 Dictionary

Abbreviation	Definition
FI	Financial Institution / organisation
DIC	Debt Information Company
TLS	Transport Layer Security
DIFI	Agency for Public Management and eGovernment
NSM	Norwegian National Security Authority
FQDN	Fully Qualified Domain Name
ETSI	The European Telecommunications Standards Institute
eIDAS	EU regulation on / a set of standards for electronic identification and trust services for electronic transactions in the European Single Market
PSD2	The EU's revised Payment Services Directive
PSD2 certificate	Qualified certificates (QWACs or QSEALCs) that are issued in compliance with ETSI TS119495 for the purposes of identification or PSPs within PSD2 access to account, as referenced in Article 34 or the Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communications
QTSPs	Qualified Trusted Service Providers (QTSPs) as described in the eIDAS regulation
QWACs	Qualified TLS Web Authentication Certificates. Identifies certificate holder, used to establis TLS connections
QSEALCs	Qualified Electronic Seal Certificate. Secures messaging.

3 Certificates

All hosted RESTful APIs must use EV (extended validation) server certificates that comply with NSM's recommendations, as described in this document.

All applications making RESTful API calls must use Enterprise Certificates (virksomhetssertifikat) as described in this document. These certificates identify businesses electronically. This gives the recipient the assurance that the sender is the one they claim to be. The certificate must be owned by the legal entity/financial institution or provider that is reporting data on their behalf.

This type of certificate (virksomhetssertifikat) conforms to Requirements specification for PKI in the public sector, Kravspesifikasjon for PKI i offentlig sektor.

* https://www.regjeringen.no/no/dokumenter/kravspesifikasjon-for-pki-i-offentlig-se/id611085/

3.1 Enrollment – Creation and signing

3.1.1 Client certificate

The ordering enterprise certificate (virksomhetssertifikat) or the person signing the agreement should have a visible role in the Brønnøysund Registry.

In addition, the client certificate shall have the following properties.

- <KeyUsage = digitalSignature> is mandatory and critical for use with Authentication in communication between FI and DIC.

Attribute for Subject->Serial number: FI's - organisation number according to ISO 6523. This organisation number will be a part of the authorization routines and must therefore match the organisation number to the legal entity/financial institution or provider.

* RFC 5280,4.2.1.3 Key Usage, https://tools.ietf.org/html/rfc5280

Financial institutions and service providers that are not registered in Norway and have no Norwegian organization number may use PSD2 compliant eIDAS client certificates provided they are both 1) QWACs compliant and 2) issued by a Qualified Trusted Service Provider (QTSPs) listed in this document.

3.1.1.1 Test and production environment

It is required that separate certificates (virksomhetssertifikat) are used for test and production.

The background for this requirement is that a certificate verification (both prod- and test) must be carried out before being activated for use in the prod- and test environment, respectively.

This requirement also helps as a safeguard against production data entering test environments, and vice versa.

3.1.2 Server certificate

All RESTful API web services hosted with FI's and DIC's must be protected with server certificates, and these certificates must comply with the requirements described here.

All server certificates to be signed with SHA-256 or a stronger algorithm, and Elliptic curve keys should be at least 256 bits in size. RSA keys should be at least 2048 bits in size, and 3072 bits if the CA can provide this.

The server certificate must be a EV (extended validation) certificate, and it has to conform to the technical specifications outlined elsewhere in this document. OV certificates that are already in use will be permitted until they expire.

In addition, the server certificates shall have the following properties:

- <ExtendedKeyUsage: **TLS Web Server Authentication**>
- <Subject Alternate Name>: **DNS:<FQDN-of-API-host>**

Non-norwegian FI's and non-norwegian service providers acting on behalf of FI's may use server certificates signed by a sertificate on Mozillas Included CA Cerficate List, provided it is an EV certificate and that all certificates in the chain adhere to the standards outlined in this document.

- https://wiki.mozilla.org/CA/Included_Certificates
- https://wiki.mozilla.org/CA/Additional_Trust_Changes

3.2 Certificate Management

3.2.1 Renewal

It is the FIs/Providers responsibility to keep track of expiration dates for its certificates and to re-new or acquire new certificates before the old ones expire.

The FIs/Providers are required to make new certificates available to all DICs for validation and testing before the old ones are retired from service, and before they expire.

The DICs can instate their own procedures detailing how this transfer is to take place. The validity and integrity of FI/Provider certificates can be checked programmatically so no special precautions are required for their transfer.

DICs are required to verify the validity of- and install these new certificates on their platform / systems and they are required to accept HTTPS requests using both the old and then new certificate until either:

1) The old certificate no longer validates (expiry/revocation).

2) The FI lets the DICs know the old certificates has been retired from use.

Timeline virksomhetssertifikat/Enterprise certificate:

- For the **test** environment the FIs/providers shall procure a new certificate and make this available to the DICs within 10 working days of expiration of the old certificate. The DICs shall validate and install said new certificate in their test environment within 5 working days of receiving it.
- For the **production** environment the FIs/providers shall procure new certificate and make this available to the DICs within 20 working days of expiration of the old certificate. The DICs shall validate and install said new certificate in their production environment within 10 working days of receiving it.

Timeline server/TLS certificate:

- For the server/TLS certificates the FIs/providers shall procure new certificate and make this available to the DICs within 20 working days of expiration of the old certificate. The DICs shall validate and install said new certificate in their production environment within 10 working days of receiving it.

The same regime will also be required for the DICs client and server certificates used in communication with Fis/Providers.

3.2.2 Revocation and maintenance

This should be done by following automated built-in mechanism to deny expired and revoked certificates like OCSP or CRL and not require manual work because it's prone to errors.

There must also be a regime for safe handling of the cryptographic material used (keys/certificates).

3.3 Use of certificates in communication between FI and DIC

For push of debt information from FI/provider to DIC in realtime.

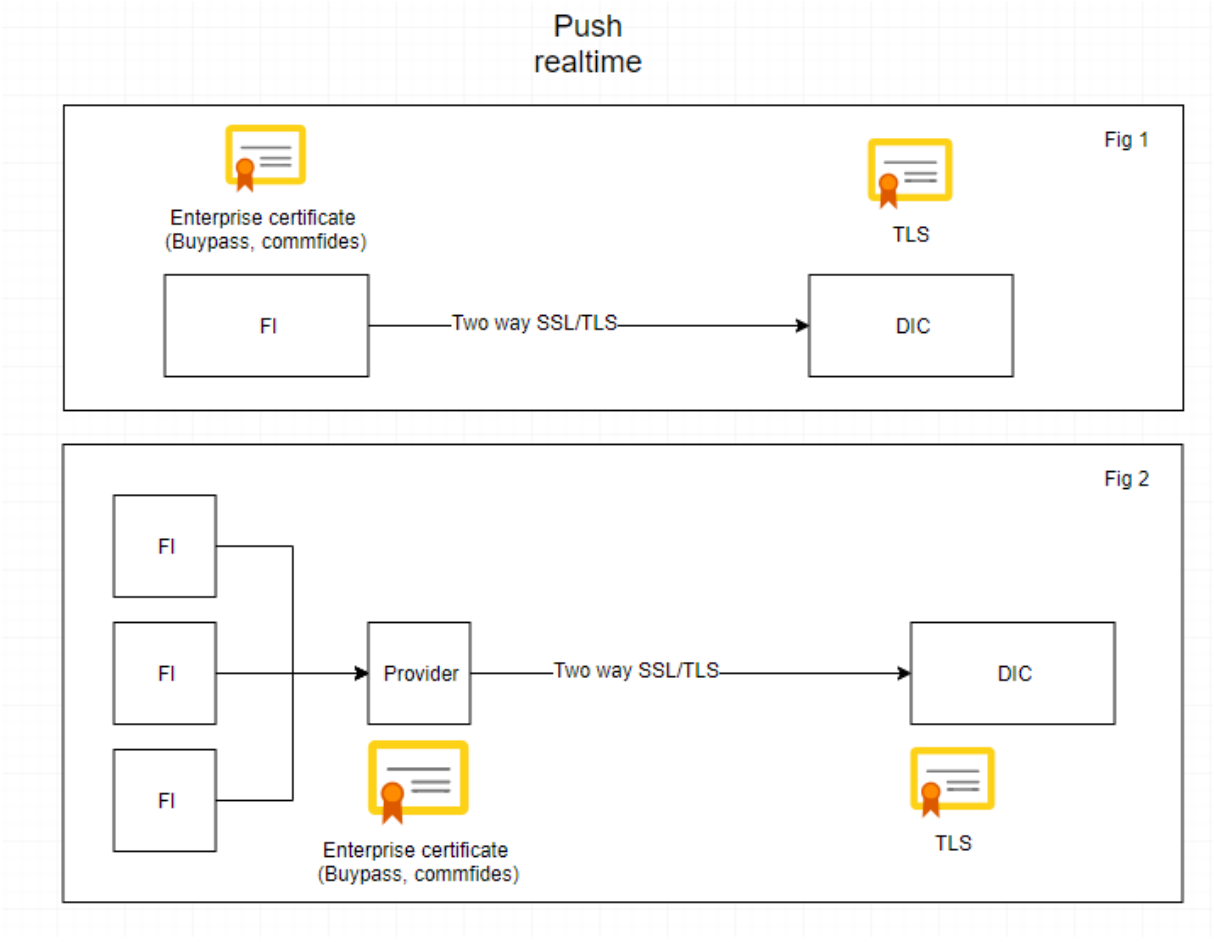


Figure 1 illustrate one FI delivers debt information by push to DIC, where FI owns the enterprise client certificate

Figure 2 illustrate one provider delivers debt information for many FIs by push to DIC, where provider owns the enterprise client certificate.

Use of certificates in communication between DIC and FI

For GET of debt information from FI/provider to DIC in batch and realtime.

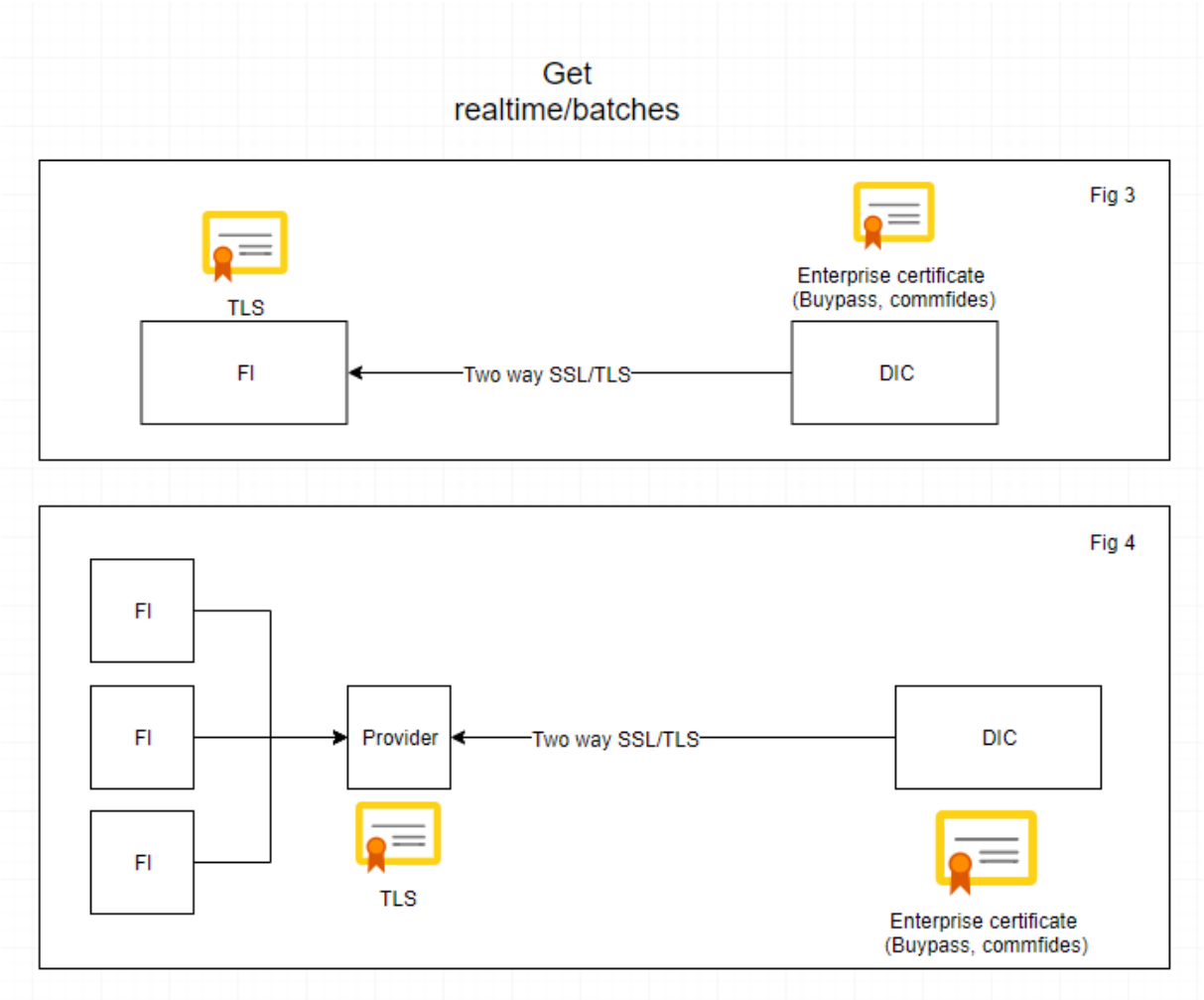
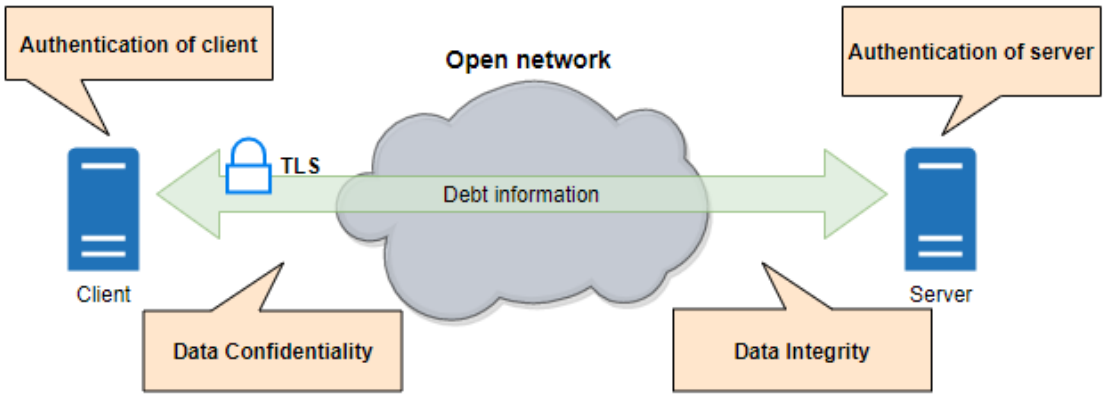


Figure 3 illustrate one DIC fetching debt information by get from FI, where DIC owns the enterprise client certificate and FI owns the TLS server certificate.

Figure 4 illustrate one DIC fetching debt information by get from Provider, where DIC owns the enterprise client certificate and provider owns the TLS server certificate.

4 HTTPS security details

Additional mechanisms for login or session handling on the application level is not necessary. Mechanisms on the transport layer is adequate. TLS with mutual authentication will be used.



4.1 Authentication of client and service

Since we are sending transactions between organizations over the internet, it is sufficient to use HTTP with TLS and mutual authentication to authenticate the client and the service, the client and server certificate is used for this. All incoming requests shall be blocked if the certificate is not approved.

4.2 Authorization of client

The client certificate used during authentication is used to authorize the client.

4.3 Confidentiality

Confidentiality between the debt information company and financial institutions is secured by HTTP over TLS.

4.4 Data integrity

Data integrity between the debt information company and financial institutions is secured by HTTP over TLS.

4.5 TLS transport requirements

Servers shall only allow TLS 1.2 or newer, and only cipher suites recommended by NSM:

https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/https.pdf

This document should be periodically reviewed and updated to reflect changes in the NSM recommendations.

5 Maintenance

Refers to compliance safety standards below:

- https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/tls.pdf
- https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/https.pdf

6 Overall security requirements

#	Requirement
SEC-01	The communication between the portal and the financial institutions shall be protected with transport layer security (TLS version 1.2). SSH shall be used for SFTP.
SEC-02	TLS with mutual authentication shall be used for web services.
SEC-03	Each portal shall have a client and server certificate for authentication.
SEC-04	Each financial institution (or their service provider) shall have a client and server certificate for authentication. A service provider may reuse a certificate for more than one financial institution.
SEC-05	Each financial institution/provider shall report which organization that is reporting data on their behalf.
SEC-06	Financial institutions shall only send and provide data to Debt Information Companies authorised by the Norwegian Ministry of Children and Equality.
SEC-07	Each financial institution is responsible for keeping certificates valid and notify Debt Information Companies about new certificates.
SEC-08	Separate certificates shall be used in test and production environment.

7 Approved Qualified Trusted Service Providers

PSD2-compliant certificates issued by one of the following QTSPs will be permitted for two way SSL authentication between FIs and DICs.

This only applies for non-norwegian FIs.

CA	Coverage	Website
Buypass	Nordic contries, Baltic states, UK, Ireland	https://www.buypass.no/
ACTALIS S.p.A.	Southern Europe	https://www.actalis.it/
certSign	Eastern Europe	https://www.certsign.ro/
D-Trust	Germany, Austria, Switzerland, BeNeLux	https://www.bundesdruckerei.de/en
Harica	Greece	https://www.harica.gr/
infocert	Spain, France, Portugal	https://infocert.digital/
Microsec	Eastern Europe	https://www.microsec.com/
Multicert	Spain, France, Portugal	https://www.multicert.com/