

B2B Security Concerns within the Automotive Industry White Paper

April 2008

Revision 20

Table of Contents

1	Overview.....	1
1.1	Introduction.....	1
1.2	Requirement.....	1
2	The Requirement.....	2
2.1	The Requirement.....	2
2.2	Document Sensitivity	2
2.3	The Internet.....	3
2.4	Security Types	3
2.5	The Three Tier model	4
3	Legality.....	5
3.1	Legal Issues.....	5
3.1.1	Legal Transaction Requirements	5
3.1.2	Current Practice	6
3.1.3	Legal Entities	7
3.2	European Law.....	7
3.2.1	The Directive	7
3.2.2	What is the legal status of electronic signatures?.....	9
3.2.3	How does an electronic signature equate to a hand-written signature?.....	9
4	The Environment	10
4.1	Networks	10
4.1.1	The Internet	10
4.2	Protocols.....	10
5	Certificates.....	12
5.1	What is a digital certificate?.....	12
5.2	How can certificates be obtained?.....	12

5.2.1	Self-Signed Certificates	13
5.2.2	Trading Partner provided certificates.....	13
5.3	Certification Authorities (CA's).....	13
5.3.1	What is a Certification Authority?	13
5.3.2	CA provided certificates.....	14
5.3.3	Can you really trust certificates issued by a CA?	14
5.3.4	Commercial CA signed Extended Validation Certificates	14
5.3.5	Which kind of certificate do I need?	15
5.3.6	Certificate Usage	15
6	The Solution.....	16
6.1	The needs of the Automotive Industry	16
6.1.1	A Secure protocol that meets the needs of the automotive industry	16
6.1.2	Certificates that meet the needs of the automotive industry.....	16
6.1.3	Why do OFTP2 users need certificates?	16
6.2	What does the Odette community require from a CA?.....	17
6.2.1	OFTP2 specific certificates	17
6.2.2	What certificate key usage is required by OFTP2?	17
6.2.3	Competent CA Operation	18
6.2.4	OFTP2 knowledge	18
6.2.5	Extended verification of certificate subscriber.....	18
6.2.6	Affordable pricing structure.....	18
6.3	How does OFTP2 solve the problem?	19
6.3.1	OFTP2 Session Security	19
6.3.2	OFTP2 File Security	19
6.3.3	OFTP2 Authentication.....	19
7	Barriers to Adoption	21

7.1	Barriers	21
7.2	Certificate Costs	21
7.3	Certificate Usage	21
7.4	Hardware Costs	21
7.5	ENX	22
7.5.1	Control by the industry	22
7.5.2	Are the original requirements for ENX still valid?	22
7.5.3	Cost Issues.....	22
7.5.4	Is ENX an expensive European solution to a global problem?	23
7.6	Proprietary OEM Certificates	23
7.7	Conformance to Standards	24
7.8	Requirement Awareness	24
7.9	Trust	24
8	Recommendations.....	25
8.1	The next step.....	25
8.1.1	Continue adoption of Security	25
8.1.2	Recommend an OFTP2 CA	25

1 Overview

1.1 *Introduction*

This paper looks at the use of digital security as it applies to the automotive sector with respect to the interaction between trading partners.

A summary of the most common security techniques is provided; discussing both the key concepts and the core underlying technologies.

The paper then attempts to identify inhibitors to the adoption of security and tables a series of possible recommendations with respect to the most suitable way forward for the automotive industry.

1.2 *Requirement*

The requirement is to securely transfer documents such as Orders, Invoices, Technical Drawings, Design specifications and Contracts between companies and the departments, individuals or functional entities which comprise the companies.

2 The Requirement

2.1 The Requirement

A solution is required which is accepted by the entire automotive community and which allows individual companies to use a single solution to securely exchange business documents with different partners on a global basis.

2.2 Document Sensitivity

We can't treat all transmitted content equally but can apply one or more of the following attributes to an item being transmitted:-

- ❑ Of no great importance. E.g. a party invitation at the successful conclusion of a joint project.
- ❑ Commercially Sensitive. E.g. Orders, Invoices and other such information that could be used by others for competitive advantage.
- ❑ Highly Commercially Sensitive. E.g. Technical drawings for the latest technological devices, possibly still in a pre-patent phase.
- ❑ Legally Restricted. E.g. Invoices that must contain certain information and increasingly be signed to prove authenticity.

Apart from legal restrictions, if the network infrastructure used for transmitting such documents is intrinsically secure, then in most cases additional security is not required.

Assuming that a secure network infrastructure that can be used for all trading partners is not available, a solution is therefore required that will allow commercially sensitive

documents to be securely exchanged with a number of different trading partners.

2.3 The Internet

The internet is the dominant and ubiquitous network that is used for networking between companies today and nobody would claim it to be anything other than insecure.

Unfortunately, there is no other cost effective alternative. Even purportedly secure virtual networks such as ENX (European Network Exchange is an association, and a Virtual Private Network, for the European Automotive industry), JNX and ANX (Japanese and US based automotive networks) run over the same back bone as the Internet, sharing the same routers, telecommunications lines and bandwidth as the internet. In the absence of a global network that is intrinsically secure, we are forced to use the existing internet network and apply our security upon it.

2.4 Security Types

There are a number of different issues with regard to securing data transmission between companies and we now need to consider the two main techniques of data security:-

- ❑ Encryption of data, used to prevent 3rd parties viewing the content.
- ❑ Digital Signatures, used to prove the authenticity of partners and ensure integrity of data.

There is a case for encryption to be used in all practicable circumstances. Encryption for non-sensitive E-mail, however, may be impractical to implement as there will be thousands of external recipients who have never considered implementing digital security.

The main trend with respect to the use of digital security between trading partners is towards the use of company certificates or server certificates to protect web exchanges by using SSL/TLS.

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers. There are slight differences between SSL and TLS, but the protocol remains substantially the same.

2.5 The Three Tier model

Security is required at all levels of a company. Certificates can be used on a:

- ❑ company basis for general purposes
- ❑ at a departmental level and
- ❑ at an individual level to provide signing and encryption capabilities for specific people within an organisation.

For example, an automotive company may utilise a certificate to secure data over the public internet. The company's engineering department may utilise their own certificate to sign and secure CAD designs and the Chief Engineer may also have his own certificate to sign and secure particularly sensitive designs.

3 **Legality**

3.1 **Legal Issues**

The legality and requirement of digital signatures is a relatively new topic.

A signature is not part of the substance of a transaction, but rather of its representation or form. Signing documents serves the following general purposes:

- ❑ **Evidence:** A signature authenticates a document by identifying the signer with the signed document. When the signer makes a mark in a distinctive manner, the document becomes attributable to the signer.
- ❑ **Ceremony:** The act of signing a document calls to the signer's attention the legal significance of the signer's act, and thereby helps prevent unconsidered engagements.
- ❑ **Approval:** In certain contexts defined by law or custom, a signature expresses the signer's approval or authorization of the document, or the signer's intention that it has legal effect.
- ❑ **Efficiency and logistics:** A signature on a written document often imparts a sense of clarity and finality to the transaction and may lessen the subsequent need to inquire beyond the face of a document. Negotiable instruments, for example, rely upon formal requirements, including a signature, for their ability to change hands with ease, rapidity, and minimal interruption.

3.1.1 **Legal Transaction Requirements**

The formal requirements for legal transactions, including the need for signatures, vary in different legal systems, and also

vary with the passage of time. There is also variation in the legal consequences of failure to cast the transaction in a required form. The statute of frauds of the common law tradition, for example, does not render a transaction invalid for lack of a "writing signed by the party to be charged," but rather makes it unenforceable in court, a distinction which has caused the practical application of the statute to be greatly limited in case law.

In recent history, most legal systems have reduced formal requirements, or at least have minimized the consequences of failure to satisfy formal requirements. Nevertheless, sound practice still calls for transactions to be formalized in a manner which assures the parties of their validity and enforceability.

3.1.2 Current Practice

In current practice, formalization usually involves documenting the transaction on paper and signing or authenticating the paper. Traditional methods, however, are undergoing fundamental change.

Documents continue to be written on paper, but sometimes merely to satisfy the need for a legally recognized form. In many instances, the information exchanged to effect a transaction never takes paper form. Computer-based information can also be utilized differently than its paper counterpart. For example, computers can "read" digital information and transform the information or take programmable actions based on the information. Information stored as bits rather than as atoms of ink and paper can travel near the speed of light, may be duplicated without limit and with insignificant cost.

Although the basic nature of transactions has not changed, the law has only begun to adapt to advances in technology. The legal and business communities must develop rules and practices which use new technology to achieve and surpass the effects historically expected from paper forms.

To achieve the general purposes of signatures outlined above, a signature must have the following attributes:

- ❑ **Signer authentication:** A signature should indicate who signed a document, message or record, and should be difficult for another person to produce without authorization.
- ❑ **Document authentication:** A signature should identify what is signed, making it impracticable to falsify or alter either the signed matter or the signature without detection.

3.1.3 Legal Entities

Certificates may be issued to entities or to individuals. As a general term, a legal entity is any entity that is recognised by law. In legal terms it is the functional entity that is important and not the individual, for example a functional entity of chief engineer may change as individuals leave a company and their successor is appointed. For this reason, certificates are often issued to functional entities, rather than to individuals.

3.2 European Law

3.2.1 The Directive

The European Directive (1999/93/EC) on a community framework for electronic signatures was published on 19 January 2000. Member States are required to implement the requirements expressed in the Directive in national legislation.

As a consequence European law recognises all electronic signatures as evidence and goes on to recognise that qualified signatures are admissible in legal proceedings.

The standards required for a qualified signature are significant: keys, software, smart-cards and every other device necessary must be of the highest level of performance and capability. This means the latest technology must be used, but it also includes using known best practices. The requirements for qualified certificates are:

- ❑ the indication that the certificate is issued as a qualified certificate;
- ❑ the identification of the Certification Authority and the State (European or foreign) in which it is established;
- ❑ the name (or pseudonym) of the signatory, to identify her/him;
- ❑ signature-verification data which correspond to signature-creation data under the control of the signatory;
- ❑ the indication of the period of validity of the certificate;
- ❑ the identity code of the certificate; and
- ❑ the advanced electronic signature of the certification-service-provider (Certification Authority).

This type of digital signature has a strong juridical value: it guarantees authentication, integrity and confidentiality whereby only the addressee can read it because the key is very difficult to decrypt. It also provides non-repudiation, where the sender can't say she didn't send the message, and the addressee can't say he didn't receive it.

The 2006 report from the European Commission on the operation of Directive 1999/93/EC states that the use of

qualified signatures has been much less than expected, mainly due to the lack of multi-application signatures, where service providers have developed solutions for their own specific services.

3.2.2 What is the legal status of electronic signatures?

Article 5.2 of the EC Directive provides for a harmonised and appropriate legal framework for the use of electronic signatures, by ensuring the recognition of all electronic signatures as evidence and admissible in legal proceedings..

This covers the full range of electronic signatures, no matter what their form or technology basis, from simple to advanced electronic signatures.

Following the EC directive in 1999, the EU implemented new complementary legislation. For example, Directive 2001/115/EC on electronic invoices recognises the validity of electronically sent invoices.

3.2.3 How does an electronic signature equate to a hand-written signature?

Article 5.1(a) of the Directive requires Member States to ensure that an Advanced Electronic Signature, which is based upon a qualified certificate and is created by a secure-signature-creation device, satisfies the legal requirements of a signature in relation to data in electronic form in the same manner as a hand written signature.

Such signatures are commonly referred to as Qualified Signatures, though this term is not expressly used in the Directive.

4 The Environment

4.1 Networks

4.1.1 The Internet

The Internet is *the de-facto* global network and companies are using the Internet for communications to take advantage of the lack of call charges and high bandwidth availability.

Unfortunately, the Internet is inherently insecure with anybody who has access to the routers being used for a connection able to look at the packets that are exchanged between computers.

It is not a safe environment for companies wishing to exchange business critical data and highly secretive information.

4.2 Protocols

The protocols used within the Automotive industry within Europe today are:-

OFTP (ODETTE File Transfer Protocol version 1)	Insecure over the internet. If used over the internet the use of a VPN is recommended.
OFTP2	Highly secure and can be used for network security, computer to computer, company to company, department to department and person to person without the need for a VPN.
FTP	Insecure over the internet. If used over the internet the use of a VPN is recommended.

S-FTP	Highly secure but can only be used for computer to computer security.
-------	---

OFTP is the dominant communication protocol used within the European Automotive industry and has been in this situation for many years. OFTP was designed to operate upon secure networks and has been traditionally implemented upon X.25 and ISDN.

OFTP2 is the security enabled variant of OFTP and is used to transmit data securely over the public internet without the need for VPNs.

5 Certificates

5.1 What is a digital certificate?

Digital certificates bind an identity to a pair of electronic keys that can be used to encrypt and sign digital information. A digital certificate makes it possible to verify someone's claim that they have the right to use a given key, helping to prevent people from using counterfeit keys to impersonate other users.

Used in conjunction with encryption, digital certificates provide a more complete security solution, assuring the identity of all parties involved in a transaction.

Digital certificates are also known as X.509 certificates as defined by ISO (International Standards Organisation).

5.2 How can certificates be obtained?

Certificates can be obtained in three different ways:

- Created by the user of a certificate, known as a self-signed certificate
- Trading Partner distribution, created by the customer for their suppliers
- Generated by a Certification Authority (CA)

The main issue relating to the provision of certificates is that of trust. Before a certificate can be accepted as trustworthy by a trading partner, the issuer of the certificate must first be trusted.

Additionally, each user should only have one certificate that is accepted by all of their trading partners, rather than being required to use a different certificate for each. Large trading partners may also maintain their own Public Key Infrastructure

(PKI) to provide certificates directly to their suppliers. A PKI is a collection of technologies, processes, and organisational policies that support the use of public key cryptography and in particular the means to verify the authenticity of public keys.

5.2.1 Self-Signed Certificates

A self-signed certificate is a certificate that is signed by its own creator, that is, the person that created the certificate also signed off on its legitimacy.

Self-signed certificates do not provide any assurance that the certificate can be trusted and is generally not regarded as an acceptable way of creating certificates.

5.2.2 Trading Partner provided certificates

In the absence of an agreed common approach to digital security some major companies have not only started issuing certificates to their suppliers, but have also inserted proprietary supplementary information into the certificate in order to make certificate usage easier within their IT systems. Although this practice may make it easier for the individual trading partner, it could render the certificate useless for use with other trading partners.

5.3 Certification Authorities (CA's)

5.3.1 What is a Certification Authority?

A certification authority (CA) is an organisation, usually commercial, which issues certificates for use by other parties. Through marketing, and audited compliance with recognised international standards, some CA's are better regarded than others.

5.3.2 CA provided certificates

A CA issues a user's certificate and then signs the certificate with the CA's own certificate; in turn the CA's certificate may be signed by another CA. Ultimately, there will be a highest-ranking CA which does not have its own certificate signed by another CA.

The value basis of obtaining a certificate from a CA (rather than using a self-signed certificate) is that the CA is widely trusted and therefore other users will implicitly trust the user's certificate. This mechanism relies upon the CA's certificate being trusted upon the computer in which the user's certificate will be used.

5.3.3 Can you really trust certificates issued by a CA?

The theory is that certificates obtained via a CA are more trustworthy than self-signed certificates, although this is misleading.

The basic certificate that may be purchased from a CA comes with little verification. Basically an email is sent back to the address of the applicant to confirm that the email address is valid, but no further checks are performed to ensure the integrity of the purchaser.

5.3.4 Commercial CA signed Extended Validation Certificates

CA's do offer additional verification services which rigorously validate any certificate request, thus providing a higher degree of trust in the certificate. These services incur a much higher cost; extended Validation certificates are available for around €700 per year.

5.3.5 Which kind of certificate do I need?

Due to the large number of certificate types that are available from CA's, it is not immediately obvious as to what kind of certificate should be purchased for use with different application purposes.

This leads to the inevitable confusion of users when deciding where to buy their certificates, it could also lead to trading partners selecting different CA's resulting in a non-standard approach.

The certificates issued by CA's vary by:

- Verification
- Type of usage, e.g.
 - Email
 - Documents
 - Network connections
 - Application program code

5.3.6 Certificate Usage

The next problem that arises with the issuing of a certificate is the definition of the function for which the certificate can be used. Typically CA's issue certificates that are either for the use of web servers to secure the connection between the client browser and the web server, or for the use of email clients to sign personal emails.

Unfortunately, even for the same type of certificates, different CA's use different key usage attributes when creating certificates.

6 The Solution

6.1 *The needs of the Automotive Industry*

6.1.1 A Secure protocol that meets the needs of the automotive industry

OFTP2 has been designed specifically to meet the security requirements of the automotive industry, whilst retaining the existing features of the first version of OFTP that has been in widespread use amongst the automotive industry for decades.

The OFTP2 has already reached RFC status (an agreed and documented internet standard) and has been adopted by a number of software vendors; the security aspects of OFTP2 are already proven and accepted by the industry.

6.1.2 Certificates that meet the needs of the automotive industry

Certificates are needed that meet the requirements of OFTP2 and that are issued by a Certificate Authority which is trusted by all automotive standards organisations, OEMs and suppliers.

The remaining issue is for the automotive community to adopt a suitable set of requirements for the issuing of certificates.

6.1.3 Why do OFTP2 users need certificates?

The security capabilities within OFTP2 utilise the PKI security mechanism which is widely regarded as the most secure mechanism that can be used for the exchange of data electronically, therefore the provision of security certificates is an intrinsic necessity for the operation of OFTP2.

6.2 What does the Odette community require from a CA?

6.2.1 OFTP2 specific certificates

Certificates can have many uses; typically certificates are available for SSL/TLS, for email signing and for data encryption. But many existing CA's do not offer certificates that cover the full breadth of features that may be employed via an OFTP2 server.

An OFTP2 server application caters for all aspects of security and therefore requires a certificate which has been created with a wide set of usage parameters. The certificate usage attributes of an OFTP2 certificate should ideally be set to include digital signature, non-repudiation, key encipherment, data encipherment, server authentication and client authentication.

This rich set of attributes therefore presents a problem for existing CA's and further illustrates the need for a CA which is able to specifically issues certificates for the use of OFTP2 applications.

6.2.2 What certificate key usage is required by OFTP2?

OFTP2 users require a flexible mechanism that will allow different certificates to be used for different purposes. For example, it may be desirable to utilise session security, but it should not be possible for the same certificate to be used to sign data.

It is quite likely for an OFTP2 server to be configured to cater for session security on a company wide basis using a single certificate, but it should not be possible to use that certificate to sign data and should be possible to utilise any number of other certificates to sign data files.

6.2.3 Competent CA Operation

The business community requires the knowledge that an OFTP2 CA is run and managed to high standards of professionalism and security. Many existing CA's are simply providing basic SSL and email certificates requiring little or no validation, which is totally unacceptable for the automotive community.

6.2.4 OFTP2 knowledge

Current CA's have little knowledge of the OFTP2 protocol or the business requirements of the automotive community. Any CA that decides to offer OFTP2 certificates must be fully capable of handling both the technical and commercial questions related to the acquisition of certificates for use within OFTP2 applications.

6.2.5 Extended verification of certificate subscriber

The current level of subscriber verification employed for most certificates is unacceptable to the automotive community and provides little benefit compared to using self-signed certificates.

The OFTP community requires that any CA's offering OFTP2 certificates should adhere to a specified minimum level of applicant verification before a certificate may be issued. This will result in a period of days before a certificate can be issued, but ensures the integrity of the OFTP2 community.

6.2.6 Affordable pricing structure

Many OFTP users are small companies with comparatively small IT budgets. It is therefore necessary for the CA's to restructure their pricing for extended verification certificates to ensure that they are affordable to the average automotive supplier.

6.3 How does OFTP2 solve the problem?

OFTP2 allows reliable, automated exchanges of business documents. OFTP2 provides three security levels:

- Session security (Network and computer to computer)
- File security
- Secure authentication (digital signatures)

6.3.1 OFTP2 Session Security

Session security encrypts an entire communications session between two trading partners so that it is not possible for a third party to view the original documents being exchanged. All protocol data units are encrypted so it is not possible to understand what protocol units are being exchanged or to examine their content. The mechanism employed by OFTP2 is the same as is used when making a secure connection (SSL/TLS) to a web site over the public internet.

6.3.2 OFTP2 File Security

File security provides an additional level of security by allowing a file to also be encrypted. This, in conjunction with session security, means that it is possible for a file to be securely exchanged between two companies, but for the file to remain encrypted until it reaches its ultimate destination such as a specific department or individual inside the recipient company.

The exchanged files can also be signed by the originator to prove the authenticity of the files.

6.3.3 OFTP2 Authentication

Secure authentication uses certificates to authenticate two communicating entities to each other. This security prevents

malicious users from connecting to an EDI server and attempting to send viruses to it or attempting to hack it.

Every trading partner uses a digital certificate, similar to the concept of someone's passport, to identify themselves. The certificate proves the holder is who they say they are, and it is up to the recipient of the communications session to accept or reject the connection based upon the credentials supplied.

7 Barriers to Adoption

7.1 Barriers

There are four main barriers to the automotive industry achieving the greatest benefit from security:

- ❑ Lack of awareness at the right level within companies
- ❑ The current CAs lack of awareness of the technical issues associated with OFTP2 security
- ❑ Misperceptions based upon the positioning of existing network solutions.
- ❑ Confusion as to the legal requirements

7.2 Certificate Costs

The high cost of certificates could be a major obstacle to the rapid uptake of OFTP2. The certificate costs imposed by existing CA's could limit the growth of OFTP2 and may not allow flexible approaches for OEM supplier bases.

7.3 Certificate Usage

The OFTP2 mechanism for the use of certificates is alien to the current usage of certificates that are provided by the CA's of today. Changes are required within existing CA infrastructures to accommodate the full spectrum of requirements that the automotive industry possesses.

7.4 Hardware Costs

For large companies, maintaining their own CA to issue certificates has a cost impact. They will have invariably left the CA creation to their specialist; at present even the lowest cost cryptographic hardware costs around 20,000 Euros.

7.5 ENX

ENX is a Virtual Private Network (VPN) that runs on top of the Internet infra-structure. Its mandate is to get data from one company to another company securely – not department to department, nor individual to individual.

7.5.1 Control by the industry

It is important that the automotive industry has control of key common services. Historically Ford, GM and Chrysler formed Covisint, but not long after it was spun off and split up. With ANX, ANXeBusiness Inc. acquired the rights to the ANX network from the Automotive Industry Action Group (AIAG) in 2001. Could the same thing happen to ENX?

7.5.2 Are the original requirements for ENX still valid?

A key original selling point of ENX was the ability to provide quality of service and bandwidth availability, but now as time has gone by both quality of service and bandwidth provided by the normal internet service providers have increased to the extent that the original requirement is no longer as much of a problem. New protocols such as OFTP2 now provide a secure internet protocol for the exchange of business sensitive data between partners.

7.5.3 Cost Issues

Compared to typical public internet access, the cost of the ENX network is high and prohibitive to many companies. Even some existing ENX users are now looking to secure transmissions over the public internet utilising protocols such as OFTP2 to overcome the complexity and cost issues related to ENX, JNX and ANX.

7.5.4 Is ENX an expensive European solution to a global problem?

ENX is primarily a European network, although ENX connections are available in some countries outside of Europe. The cost of ENX connections in South America is prohibitive to most suppliers. The equivalent secure network in the USA is called ANX, but it is interesting to note that there is no secure connection between the ENX and ANX networks thereby resulting in a purely European solution to secure business connections to a global automotive industry.

Connection to the ENX network is via routers provided and configured by ENX Internet Service Providers (ISP). Each company to company connection necessitates the need for a change to the routers configuration, which is managed by the small number of ENX ISP's. The centralised nature of this environment provides a single point of failure which could result in the loss of the entire ENX network.

7.6 Proprietary OEM Certificates

Some OEM's create certificates with non-standard content that is used by their internal applications. Suppliers must therefore use the certificates issued by the OEM and cannot use standardised certificates.

The consequence is that a supplier must maintain multiple certificates, but which ones, if any, are legal? Those acknowledged by a governmental organisation as being legal in the context of their usage are obviously legal. But where do self-signed certificates signed by a customer stand?

Does a certificate for a supplier or an entity within a supplier, signed by the customer have a meaning? The answer is "yes" for the customer and also "yes" for third parties if the customers root certificate is generally available and if the

customer is regarded as trustworthy. This type of trust is a clique trust, i.e. a trust within a group of friends.

7.7 Conformance to Standards

The issue is also one of standards and conformance to standards. Being different can sometimes give a company a proprietary and commercial advantage, but in other cases being different can have an adverse effect which can negatively impact the industry as a whole.

7.8 Requirement Awareness

Any, if not most, security specialists in the OEMs have up to now only been required to focus upon the more traditional areas of certificate usage such as SSL/TLS and signed emails. Education is required to ensure that OEMs understand the full range of security features offered by OFTP2 and the implications upon the type of certificates required.

7.9 Trust

Among other things, it requires some root of trust. Somewhere in the system there must be one or more trusted parties; authorities that can then certify, using encryption, other, lesser entities. One very difficult question is, who should be the certifying authority?

8 Recommendations

8.1 *The next step*

The automotive community is now ideally placed to reap the financial benefits of a secure global network that can be used to exchange business documents between trading partners.

8.1.1 Continue adoption of Security

The automotive community must continue the adoption of the OFTP2 protocol as the protocol of choice. The combination of the internet and OFTP2 provides the automotive industry with a secure, low cost, global network that can be used for the exchange of documents with all trading partners.

8.1.2 Recommend an OFTP2 CA

A CA must be chosen to lead the deployment of certificates that meets the requirements of the automotive industry, but the existing CA's within the market place do not satisfy these requirements for the reasons already given.

A CA must therefore be recommended to the automotive industry by the automotive standards organisations (e.g. Odette International, AIAG, etc.). It is vital that the OEM's together adopt a stance towards acceptable certificates in order to allow the global adoption of OFTP2.