It’s a matter of trust!

Regardless of the industry hype surrounding the emergence of NFC, like any other technology, it will not achieve its full potential and market penetration unless consumers have confidence in it. So what can we do to build that confidence?

Near Field Communications (NFC) has huge potential, it is a truly disruptive technology and will not only change the way consumers interact with objects, but also allow them to interact with objects that they have been unable to do so with before. This type of disruption inevitably generates some level of scepticism and naturally leads to cautious behaviour. It is important that the NFC industry does what it can to alleviate this scepticism by building confidence in the technology.

Let’s look at a simple example: imagine you are walking down the street and you see an advertisement for a concert you would like to attend, before the arrival of NFC you would very likely have had to remember a website address that you would look at later but now you can simply touch your NFC phone on the poster and go straight to the website to buy tickets – wonderful!!

But the question is would you touch it? Before you touch the poster you are going to make a largely subconscious decision as to whether you trust the technology to do what you expect. Many different factors will affect your decision. A major part of your decision making process will be based on ‘can you be sure that touching the NFC tag will take you to the website you expect’ or is it going to take you unwittingly to a different site that may be malicious. If consumers have doubts they will be less likely to use the technology.

Posters equipped with NFC tags, often referred to as ‘Smart posters’, could be susceptible to a variety of threats. The types of threat that NFC enabled posters might be prone to include:

- Data modification – the URL of a website or the number to which a SMS is to be sent could be changed
- Tag replacement – an existing tag could be replaced by a malicious one

Data modification is fairly easily overcome by locking the tag. Performing this action makes it impossible for the data in the tag to be changed. This locking is typically done by the company which is providing the tag programming before the poster is deployed.

Modifying the data in a tag or replacing a tag with another one could open up a number of possible threats. If one can replace, for example, the URL in a tag then the user could be unknowingly directed to a malicious web application which could be used to download malicious software to the mobile device which might, for example, track users actions or capture personal information, this malicious web application could then very quickly redirect the user to the original webpage so that they are

© NFS 2017

completely unaware of what has happened. As commented above it is fairly easy to prevent modification of data in tags by locking them but the surreptitious replacement of one tag by another is a little more challenging to overcome.....

To overcome tag replacement we need a mechanism which can clearly indicate to the user that they can trust the contents of the NFC tag before they actually accept it and trigger the corresponding action. Fortunately the NFC Forum has defined a basic framework which will allow us to do this.

This framework takes the form of the Signature RTD (Record Type Definition). The Signature RTD defines a mechanism for attaching a digital signature and certificate to NFC content when it is written in to an NFC tag. If the data in the tag is subsequently altered or replaced the signature will not be verifiable and so the user can be informed that the tag contents are not authentic.

The Signature RTD describes how we can append a digital signature and certificate to the end of a NDEF (NFC Data Exchange Format) message.

A NDEF message carrying a website URL without a signature takes the form:

NDEF Header	Type len	Payload len	"U"	www.somesite.com

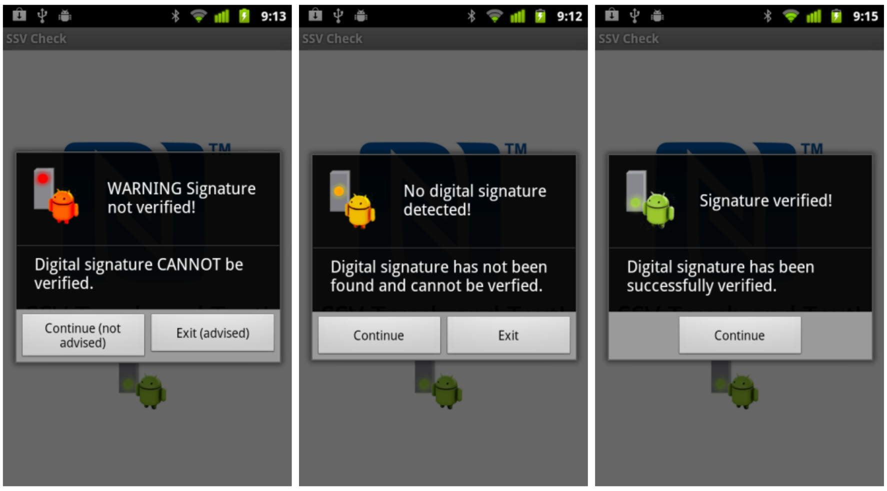
When a signature is attached the format becomes:

NDEF Header	Type len	Payload len	"U"	www.somesite.com	NDEF Header	Type len	Payload len	"Sig"	signature + certificate

When this NDEF message is read by a mobile phone the phone would first check that the certificate is valid and issued by a trusted organisation, the name given to this trusted organisation is ‘Certificate Authority’. If the certificate is valid, the mobile phone then extracts a public key from the certificate and uses that to decrypt the signature and check its validity. This framework provides a mechanism to detect alterations to tag data or the presence of uncertified data which can then be indicated to the user.

An important aspect in building trust and confidence is providing a consistent user experience so that no matter where the person is and regardless of which phone they are using they recognise the information they are being given. Furthermore, we need to see ubiquitous support for the signature RTD across all devices along with a common set of certificates used to authenticate the signature. This ubiquitous support is not yet in place but with co-operation between key players in the NFC industry it can be achieved. In the NFC eco-system the mobile device makers are ultimately responsible for implementing the functionality we all use but other players can influence what goes into each phone. The Mobile Network Operators (MNO’s) have considerable influence and therefore they are well placed to influence requirements for new functionality. Trade associations such as the NFC Forum also have a valuable part to play although it is not typical for the NFC Forum to involve themselves in the user interface requirements.

When a consumer touches their phone on the poster the phone can check the validity of the signature and indicate the status of that signature to the user through a simple visual scheme such as:



WARNING Signature not verified!

Digital signature CANNOT be verified.

No digital signature detected!

Digital signature has not been found and cannot be verfied.

Signature verified!

Digital signature has been successfully verified.

This principle will give the user an immediate indication of the authenticity of the tag contents and, in the case of a green light, the confidence to continue the interaction. The use of red, amber and green lights is almost universally recognisable.

So far we have looked at the tools we have at our disposal to provide secure and trusted applications let's now look at how these tools can be used in real applications. To provide a system which is trustworthy the signature must be created by a trusted entity which can also attach a verifiable certificate. If both of these components are in place the mobile device can verify the authenticity of the data. The organisation providing this signing process could be considered as a 'Trusted Application Manager' in that it is an entity which the industry and public trust and it manages the signing and authenticity of the data for NFC applications.

The Trusted Application Managers provide a security service to NFC application providers but unlike the much discussed TSMs (Trusted Service Managers) the Trusted Application Manager offers an 'offline' service. The usual TSM acts in more of an inline way such that they sit between the NFC service provider and the user to provide secure application loading and management on mobile devices. They can also provide security for each individual transaction particularly when looking at payment and ticketing applications; by contrast the Trusted Application Manager offers a one time only security service through the signing of the NDEF data. Once the tag is deployed the Trusted Application Manager essentially plays no further part.

When a company wishes to deploy NFC posters it first needs to decide what it would like the tag to do, for example; direct the user to a website, send an SMS or make a call. Once the action is decided upon it can then create a suitably formatted NDEF message ready to write to a tag. To add the signature it

© NFS 2017

will then submit the NDEF message to the Trusted Application Manager; thereafter the Trusted Application Managers sign the NDEF message. As an additional service the Trusted Application Manager may offer to create the NDEF Message from a website URL, SMS message or phone number directly thereby offering a one-stop solution. Before signing the NDEF message the Trusted Application Manager will have verified the authenticity of the company deploying the posters through an appropriate process of due diligence much the same as when SSL certificates are issued. Once processed by the Trusted Application Manager the resulting signed message can then be written to the tag(s) and deployed in posters. It is worth re-iterating that the signature created by the Trusted Application Manager is unique to that particular NDEF message so if the company deploying the posters wants several different actions to be performed by different posters then they must submit each message for signing separately.

The role of Trusted Application Manager could be performed by many different organisations. It is expected that established security based companies such as those currently issuing SSL certificates for web applications could expand their offering to include NFC, many of these are well placed to do so as they already act as Certificate Authorities and hence are able to issue NFC certificates within their existing infrastructure. We might also expect new entrants into this market coming from an NFC background although the challenge of creating a trusted brand should not be under estimated.

From what we have discussed so far we can now see how the authenticity of data on a tag can be assured by adding a digital signature, and we understand the procedure for creating that signature and writing it to a tag(s). We can now look at the verifying of a signature when it is read by a mobile device.

When a mobile device reads the NDEF message from a tag it will detect that a signature is attached, the procedure for verifying the signature starts with the checking of the authenticity of the certificate which is also attached.

Certificates are verified through a chain of trust. The trust for the certificate is often described as the trust anchor and is defined as the ‘Root Certificate Authority’. A certificate authority can issue many certificates that take the form of a tree structure. A root certificate is the top-most certificate of the tree and is deemed as fully trustworthy.

All certificates immediately below the root certificate inherit the trustworthiness of the root certificate. In mobile devices it is typically that one of these lower ‘subordinate’ certificates which is installed in the device but as it inherits the trustworthiness of the root certificate it becomes ‘trusted’.

Contained within this subordinate certificate is a key which can be used to decrypt the certificate attached to the NDEF message and verify, through an embedded signature, that the certificate has not been tampered with. If the certificate is authentic a further key can be extracted from it, this key is then used to decrypt the signature attached to the NDEF message. The signature is typically a ‘hash’ of the NDEF data created using algorithms such as MD5 or SHA-1, the mobile device can now perform the same hash of the NDEF data and compare the results with the decrypted signature, if they match

© NFS 2017

then the NDEF message is unaltered and can be considered to have been authenticated allowing the user to continue with increased confidence.

As we have discussed above; building trust in NFC applications is essential if it is to realise its potential. By using the framework described above when deploying NFC content we can provide a solution which will help to build trust in NFC applications thereby encouraging the users to interact with NFC posters. Mobile device makers have already invested massively in the development of NFC enabled devices however the industry needs them to continue to develop these platforms adding support for systems such as the Signature RTD and to work together to agree a consistent user experience. We also need to encourage the establishment of Trusted Application Managers to provide the secure link between NFC applications and the users.

____

Written by Glenn Needham, Director of Near Field Solutions Ltd

Glenn is a recognised authority on NFC and contactless technology having been involved in the development of NFC and contactless products and applications for many years. He was formally the chair of the NFC Forum Security Working Group. He is a member of the UK panel for the International Standards Organisation related to contactless and RFiD topics and is an active member of the European Telecommunications Standards Institute Smartcard Project Technical Body.

www.usingnfc.com

+44 (0)115 922 5479

© NFS 2017