Dr. Jon's Wireless Security

Cellular Networking Perspectives

Editor: David Crowe Vol. 1, No. 5 July, 1999

The Crypto-Answer Man

This month we are giving Dr. Jon Hamilton a break. Instead, we have invited the *Crypto Answer Man* to fill our pages. This cryptology expert, who prefers to remain anonymous, will be answering questions for Dr. Jon's Wireless Security or our website (www.cnp-wireless.com/cryptoqa.html). His articles will later be published, in condensed form, on our website.

Transmitting Keys Over a Radio Interface

***Q*:** How can you securely transmit a secret key over a radio interface?

Alan Turing

***A*:** A very good question! This is especially important today in the world of ubiquitous wireless communications. One way to securely transmit a secret key is to not actually transmit it at all. Instead have the communicants (i.e. the two parties attempting to exchange the key) independently derive it on both sides of the radio interface. That is, let our well-known friends Alice and Bob (or two radio devices) solve the key management problem without sharing any secret information using a key agreement protocol. The first and best known of these is the Diffie-Hellman Key Exchange (also called exponential key exchange).

Simple put, for Diffie-Hellman key exchange, Alice selects a large prime number (p) at least 512 bits in length. She also chooses another number that is less than the first (α). She then sends these two values to Bob. Next both Alice and Bob independently select their own secret random numbers (a and b), also at least 512-bits long. They then commence to perform modular exponentiation with their secret numbers and the public numbers. That is, they calculate:

α^a modulo p (Alice)
α^b modulo p (Bob)

They then exchange the results of these calculations and perform another calculation using the other's numbers. Upon completing this second computation, Alice and Bob have identical results and a shared key: $K = \alpha^{a\,b} \bmod p$. In doing this, Alice and Bob have generated a key that they both know and no one else can figure out based on the information that was sent between them. The security of the system rests on the intractability of computing discrete logarithms.

AHAG Update

The AHAG will be allowing proponents of various ESA and ESP proponents to present their ideas the day before the August 30-31, 1999 meeting in Toronto, Canada.

An AHAG proposal to insist that home systems share session keys with serving systems is rubbing the carriers the wrong way, as they fear they will lose control and potentially expose key information unnecessarily. On the other hand, is SS7 capable of carrying the larger keys that will be required for ESA and ESP?

About *Dr. Jon's Wireless Security*

Price

The stand-alone subscription price for *Dr. Jon's Wireless Security* is 75% of the cost of the corresponding *Cellular Networking Perspectives* subscription (e.g. $225 for a basic subscription).

Current subscribers to *Cellular Networking Perspectives* can extend their subscription to include *Dr. Jon's Wireless Security* for only a 50% premium over their current *Cellular Networking Perspectives* subscription price. For example, subscribers to our standard 10-copy license paying $300 per year for *Cellular Networking Perspectives* would pay only an additional $150 per year for *Dr. Jon's Wireless Security*.

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Month's Major Topic

Wireless Network Security Issues. Updates on ESA and ESP.

Next Issue Due…

August 17th, 1999.

Future Topics

Interim CAVE • Global Authentication • UIM • Export Control Laws • ESA/ESP Implementation Guidelines

Dr. Jon's Wireless Security is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary AB, T2N 3W1, Canada.
Contact Information: Phone: 1-800-633-5514 (+1-403-274-4749) **Fax:** +1-403-289-6658 **Email:** cnpsales@cnp-wireless.com **Web:** http:/www.cnp-wireless.com/djws.html.
Subscriptions: $150 for current *Cellular Networking Perspectives* subscribers for delivery in the USA or Canada, US$200 elsewhere. Non-subscribers pay $225/yr. for delivery in the USA or Canada, US$300/yr. elsewhere. Payment is accepted by cheque, bank transfer, American Express, MasterCard or Visa. **Delivery:** Email or 1st class mail.
Back Issues: Available individually for $20 in the US and Canada and US$25 elsewhere, or in bulk at reduced rates. **Discounts:** Educational and small business discount: 25% off any order. **Copies:** Each subscriber is licensed to make up to 10 copies of each issue or back issue. Please call for rates to allow more copies.

Encryption Certificates

Q: What are encryption certificates? And, how does the certificate authority authenticate the party it sends a certificate to?

Ben Levitan, GTE TSI

A: Encryption certificates are useful in public key cryptology (PKC), also known as asymmetric key cryptography. The public-key is required for the following security services:

1. Validation of digital signatures and
2. Encryption of session encryption (conventional or private) keys.

For example, if Alice wants to verify the digital signature of Bob, she needs his public key. Also, Alice must provide her public key to Bob so he can encrypt a message to her.

This generates a fundamental question:

What happens if Alice's public key is replaced by another persons?

This presents a significant problem – in fact, a major vulnerability with non-certificate-based Private-Key cryptography.

Certificate Authorities

In certificate-based Public Key cryptography, the public key certificate is essentially the public key of someone that is digitally signed by a trustworthy person. In this way, the certificate provide a means to prevent an adversary from substituting one public key for another.

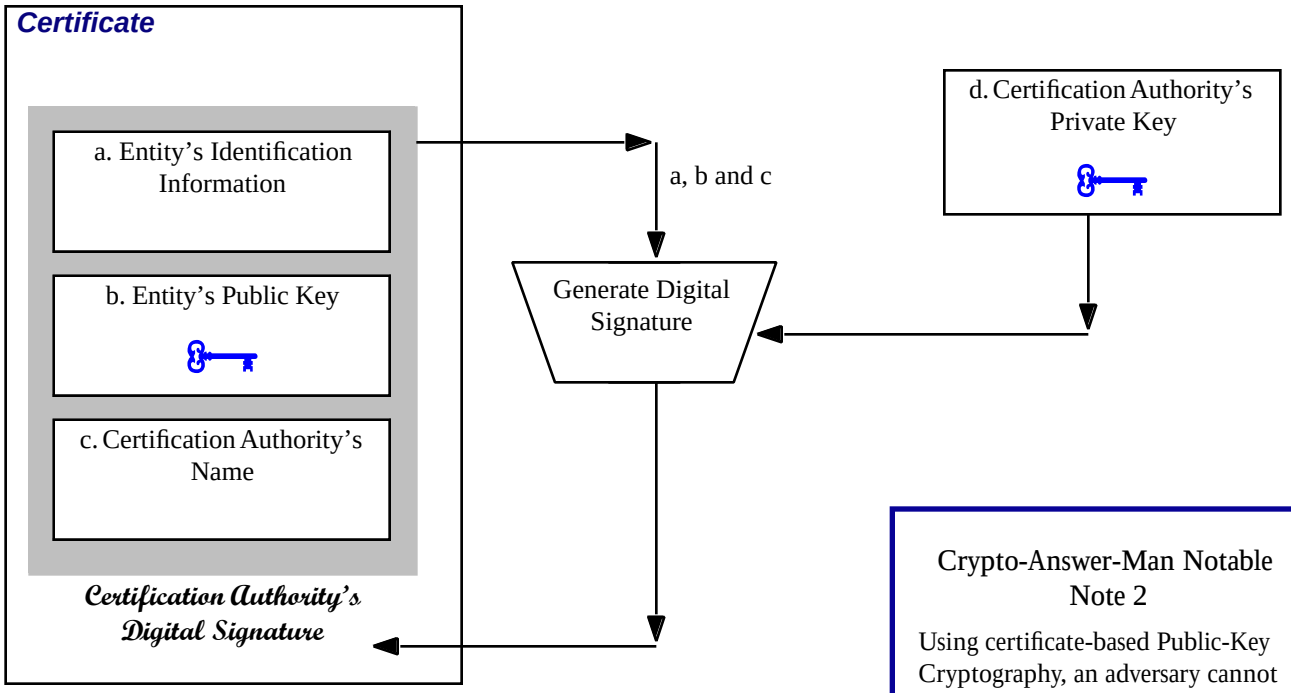
A certification authority issues certificates for a community of public-private key-pair users. Remember that in public-key cryptography, each communicant or user is assigned two keys: a secret key and a public key (hence the name asymmetric key cryptography). The user's 'credentials' are bound by the signature of the certification authority. The general structure of a certificate is shown in Figure 1.

As shown, the entity's (Alice, for example) information, public key and the name of the Certificate Authority are digitally signed to form a certificate. For the signing process the private key of the Certificate Authority, kept securely by the Certificate Authority, is used.

Crypto-Answer-Man Notable Note 1

A *certificate* contains a public key that is securely associated with an entity (e.g., person, device, etc.). The certificate, by means of a digital signature of a trusted entity (called a certification authority or CA), binds the entity to the key.

Figure 1: Simple Public-Key Certificate



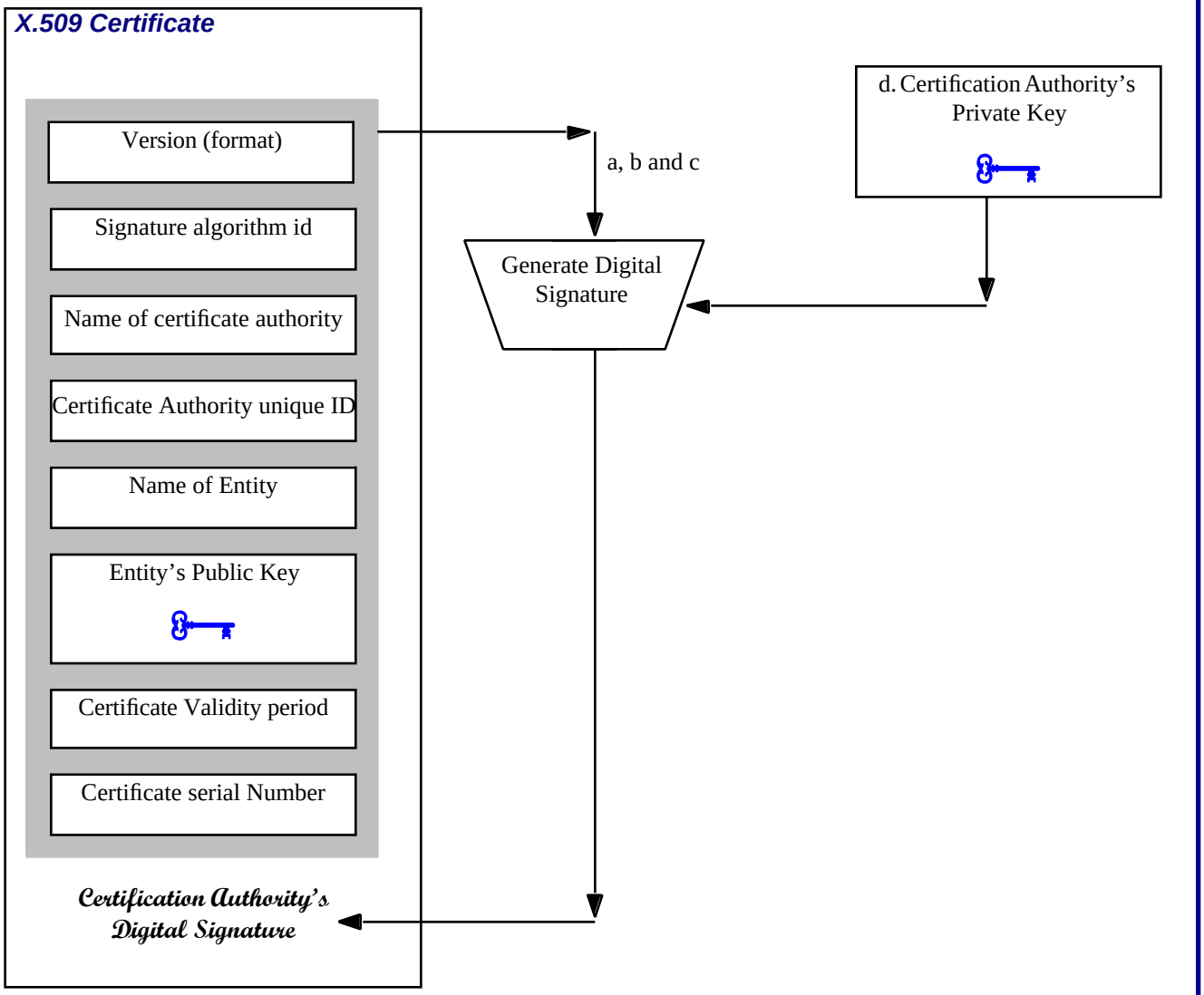
X.509 Certificate Directories

The ITU (International Telecommunication Union) and ISO (International Organization for Standardization) developed a comprehensive directory service technology in the mid-1980's. These directory standards, known as X.500, provide the basis for constructing a multi-purpose directory service for organizations

Crypto-Answer-Man Notable Note 2

Using certificate-based Public-Key Cryptography, an adversary cannot substitute another public key and thereby circumvent the cryptographic security. That is, the adversary cannot disclose an encrypted message to unauthorized parties and cannot forge signatures.

Figure 2: X.509 Certificate Structure



world-wide. The security standards within the ISO framework, known as the X.509 standards, include specifications for public-key certificates. The structure of an X.509 certificate is shown in Figure 2.

The X.509 certificate is a collection of fields or attributes that have been bound by the signature of a known and 'trusted' Certificate Authority. Even with all its complexity, the X.509 certificate, like all certificates, contains three primary parts:

1. Entity public key,
2. Entity attributes (name, serial number, etc.), and
3. Certificate Authority signature.

Authenticating the Recipient

On to Ben's second question - How does the certificate authority authenticate the party it sends a certificate to?

Well, the Certificate Authority-User dialogue must occur through traditional out-of-band channels. For instance, Alice (the entity) could visit a notary public and present a birth certificate or other identifying information in person. The notary provides Alice a secret passphrase that may later be used for an online communication with the Certificate Authority to request the certificate.

This means that even certificate authorities are subject to identification fraud, also known as 'social engineering'. If Sally can persuade the notary that she is really Alice, she may still be able to fraudulently obtain a certificate!

Crypto-Answer-Man Notable Note 3

Not only is certificate-based Private-Key Cryptography rather complex from a business, technical, social and legal standpoint, it is also very hot! Although only one small component, it provides the critical foundation for electronic commerce, e-business and public-key infrastructure, today and in the future.