**MODULE 4 & 5**

1. This short note offers a quick overview of voice communications using internet technology to carry the voice signal. The purpose is to assist a public policy decision maker who wishes to understand some of the current debate regarding VoIP. The main point is: the phrase voice over internet protocol (VoIP) is deceptively simple. VoIP refers to dozens of activities that differ greatly in their quality, cost, and relationship to traditional regulatory boundaries.
2. Data communications over the Internet relies on dozens of protocols—rules defining the required steps for a communications task. For example, part of the protocol for telephone calls includes (1) waiting for dial tone before dialing and (2) the different sounds that indicate that the called telephone is either ringing or busy. The internet protocol (IP) is the basic protocol at the heart of the Internet. An IP message is the data communications equivalent of a postcard—it carries the recipient’s and sender’s addresses, a block of data, and little else. Other protocols, such as TCP and HTTP, build on IP to create additional capabilities.
3. Data communications over the Internet relies on dozens of protocols—rules defining the required steps for a communications task. For example, part of the protocol for telephone calls includes (1) waiting for dial tone before dialing and (2) the different sounds that indicate that the called telephone is either ringing or busy. The internet protocol (IP) is the basic protocol at the heart of the Internet. An IP message is the data communications equivalent of a postcard—it carries the recipient’s and sender’s addresses, a block of data, and little else. Other protocols, such as TCP and HTTP, build on IP to create additional capabilities.
4. **PVDM** stands for packet voice DSP module; it is the Cisco product name for the module that provides digital signal processing resources to a system. DSP stands for Digital Signal Processor; it is a generic Industry terminology. A **PVDM** module could be staffed with one or multiple DSPs
5. Gateways allow VoIP telephones to receive calls dialed to telephone numbers and permit VoIP telephones to place calls to traditional telephones. That is, a gateway permits a telephone number to be associated with a specific VoIP user
6. The Resource Reservation Protocol is a transport layer protocol designed to reserve resources across a network for quality of service using the integrated services model. RSVP operates over an IPv4 or IPv6 and provides receiver-initiated setup of resource reservations for multicast or unicast data flows
7. the impact of heterogeneous receivers on the throughput of multicast flow control and propose a new multicast flow control algorithm to optimally partition group members into multiple subgroups.
8. Multiprotocol Label Switching (**MPLS**) is a type of data-carrying technique for high-performance telecommunications networks. **MPLS** directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table.
9. The Real-Time Transport **Protocol** (**RTP**) is an Internet **protocol** standard that specifies a way for programs to manage the real-time transmission of multimedia data over either unicast or multicast network services.
10. <https://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol>
11. <https://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol>
12. <https://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol>
13. <https://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol>
14. <https://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol>
15. <https://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol>
16. <https://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol>
17. <https://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol>
18. <https://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol>
19. <https://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol>
20. <https://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol>

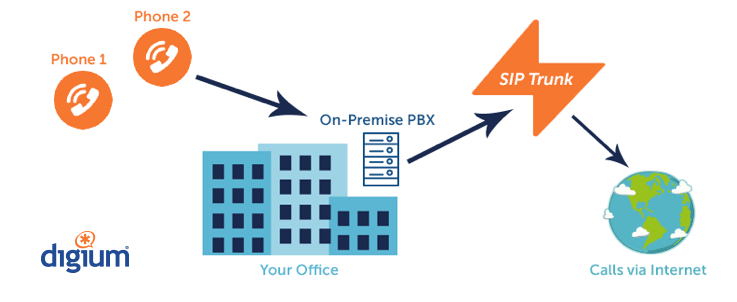
**MODULE 4 & 5**

1. <https://bear.warrington.ufl.edu/centers/purc/docs//PRESENTATIONS/events/2004_annual_conference/adddocs/0204_Jackson_A_Quick_Introduction.pdf>
2. <https://bear.warrington.ufl.edu/centers/purc/docs//PRESENTATIONS/events/2004_annual_conference/adddocs/0204_Jackson_A_Quick_Introduction.pdf>
3. <https://bear.warrington.ufl.edu/centers/purc/docs//PRESENTATIONS/events/2004_annual_conference/adddocs/0204_Jackson_A_Quick_Introduction.pdf>
4. <https://bear.warrington.ufl.edu/centers/purc/docs//PRESENTATIONS/events/2004_annual_conference/adddocs/0204_Jackson_A_Quick_Introduction.pdf>
5. <https://bear.warrington.ufl.edu/centers/purc/docs//PRESENTATIONS/events/2004_annual_conference/adddocs/0204_Jackson_A_Quick_Introduction.pdf>
6. <https://microsoft.github.io/language-server-protocol/>
7. <https://microsoft.github.io/language-server-protocol/>
8. <https://microsoft.github.io/language-server-protocol/>
9. <https://microsoft.github.io/language-server-protocol/>
10. <https://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol>
11. <https://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol>
12. <https://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol>
13. <https://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol>
14. <https://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol>
15. <https://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol>

**MODULE 4 & 5**

1. SIP trunking works with **VoIP phone systems (Voice Over Internet Protocol)** and is based on **SIP (Session Initiation Protocol)**.

SIP, which is the basis of SIP Trunking, is the standard communications protocol for voice and video in a **Unified Communications (UC)** solution across a data network.



SIP Trunking eliminates the physical connection to a phone company. There are no hardware, wiring, or circuit boxes to maintain for connection to the PSTN (phone service provider).

A SIP “trunk” is installed virtually over your business’s existing internet connection, therefore replacing the need for traditional analog phone lines.

Reducing multiple phone lines into a single point of entry drastically reduce charges for incoming lines and the IT cost associated with the maintenance of those lines. (Some organizations prefer to maintain standard lines for faxes and alarms.)

A phone number, or **Direct Inward Dialing number (DID)**, is less expensive when purchased with a SIP Trunk.

Traditionally, when a DID is obtained from a phone company, charges are applied for the DID, IT and maintenance services, and the hardware connecting the shared physical lines or channels. A DID provided without these infrastructure costs is more affordable.



The *Resource Reservation Protocol (RSVP)* is a network-control protocol that enables Internet

applications to obtain differing qualities of service (QoS) for their data flows. Such a capability

recognizes that different applications have different network performance requirements. Some

applications, including the more traditional interactive and batch applications, require reliable delivery

of data but do not impose any stringent requirements for the timeliness of delivery. Newer application

types, including videoconferencing, IP telephony, and other forms of multimedia communications

require almost the exact opposite: Data delivery must be timely but not necessarily reliable. Thus, RSVP

was intended to provide IP networks with the capability to support the divergent performance

requirements of differing application types.

It is important to note that RSVP is not a routing protocol. RSVP works in conjunction with routing

protocols and installs the equivalent of dynamic access lists along the routes that routing protocols

calculate. Thus, implementing RSVP in an existing network does not require migration to a new routing

protocol.

Researchers at the University of Southern California (USC) Information Sciences Institute (ISI) and

Xerox’s Palo Alto Research Center (PARC) originally conceived RSVP. The Internet Engineering Task

Force (IETF) subsequently specified an open version of RSVP in its RFC 2205 based directly on the

USC and PARC version. RSVP operational topics discussed in this chapter include data flows, quality

of service, session startup, reservation style, and soft state implementation. Figure 48-1 illustrates an

RSVP environment.

1. <http://faculty.kfupm.edu.sa/coe/marwan/richfiles/Chapter%2048%20(Resource%20Reservation%20Protocol).pdf>
2. <http://faculty.kfupm.edu.sa/coe/marwan/richfiles/Chapter%2048%20(Resource%20Reservation%20Protocol).pdf>
3. <https://www.adobe.com/digitalimag/pdfs/about_metadata.pdf>
4. <https://www.adobe.com/digitalimag/pdfs/about_metadata.pdf>

The most distinct feature of Public Key Infrastructure (PKI) is that it uses a pair of keys to achieve the underlying security service. The key pair comprises of private key and public key.

Since the public keys are in open domain, they are likely to be abused. It is, thus, necessary to establish and maintain some kind of trusted infrastructure to manage these keys.

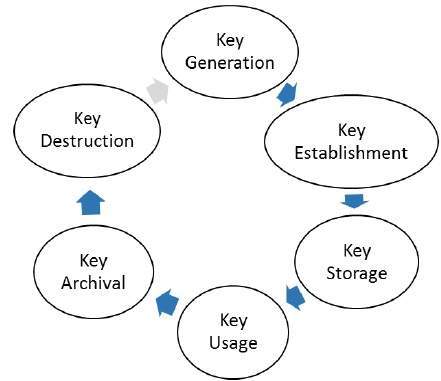
Key Management

It goes without saying that the security of any cryptosystem depends upon how securely its keys are managed. Without secure procedures for the handling of cryptographic keys, the benefits of the use of strong cryptographic schemes are potentially lost.

It is observed that cryptographic schemes are rarely compromised through weaknesses in their design. However, they are often compromised through poor key management.

There are some important aspects of key management which are as follows −

* Cryptographic keys are nothing but special pieces of data. Key management refers to the secure administration of cryptographic keys.
* Key management deals with entire key lifecycle as depicted in the following illustration −



* There are two specific requirements of key management for public key cryptography.
  + **Secrecy of private keys.** Throughout the key lifecycle, secret keys must remain secret from all parties except those who are owner and are authorized to use them.
  + **Assurance of public keys.** In public key cryptography, the public keys are in open domain and seen as public pieces of data. By default there are no assurances of whether a public key is correct, with whom it can be associated, or what it can be used for. Thus key management of public keys needs to focus much more explicitly on assurance of purpose of public keys.

The most crucial requirement of ‘assurance of public key’ can be achieved through the public-key infrastructure (PKI), a key management systems for supporting public-key cryptography.

Public Key Infrastructure (PKI)

PKI provides assurance of public key. It provides the identification of public keys and their distribution. An anatomy of PKI comprises of the following components.

* Public Key Certificate, commonly referred to as ‘digital certificate’.
* Private Key tokens.
* Certification Authority.
* Registration Authority.
* Certificate Management System.

Digital Certificate

For analogy, a certificate can be considered as the ID card issued to the person. People use ID cards such as a driver's license, passport to prove their identity. A digital certificate does the same basic thing in the electronic world, but with one difference.

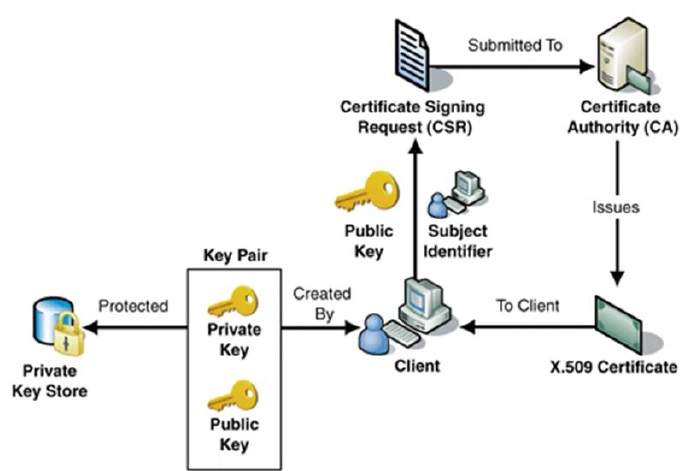
Digital Certificates are not only issued to people but they can be issued to computers, software packages or anything else that need to prove the identity in the electronic world.

* Digital certificates are based on the ITU standard X.509 which defines a standard certificate format for public key certificates and certification validation. Hence digital certificates are sometimes also referred to as X.509 certificates.

Public key pertaining to the user client is stored in digital certificates by The Certification Authority (CA) along with other relevant information such as client information, expiration date, usage, issuer etc.

* CA digitally signs this entire information and includes digital signature in the certificate.
* Anyone who needs the assurance about the public key and associated information of client, he carries out the signature validation process using CA’s public key. Successful validation assures that the public key given in the certificate belongs to the person whose details are given in the certificate.

The process of obtaining Digital Certificate by a person/entity is depicted in the following illustration.



As shown in the illustration, the CA accepts the application from a client to certify his public key. The CA, after duly verifying identity of client, issues a digital certificate to that client.

Certifying Authority (CA)

As discussed above, the CA issues certificate to a client and assist other users to verify the certificate. The CA takes responsibility for identifying correctly the identity of the client asking for a certificate to be issued, and ensures that the information contained within the certificate is correct and digitally signs it.

Key Functions of CA

The key functions of a CA are as follows −

* **Generating key pairs** − The CA may generate a key pair independently or jointly with the client.
* **Issuing digital certificates** − The CA could be thought of as the PKI equivalent of a passport agency − the CA issues a certificate after client provides the credentials to confirm his identity. The CA then signs the certificate to prevent modification of the details contained in the certificate.
* **Publishing Certificates** − The CA need to publish certificates so that users can find them. There are two ways of achieving this. One is to publish certificates in the equivalent of an electronic telephone directory. The other is to send your certificate out to those people you think might need it by one means or another.
* **Verifying Certificates** − The CA makes its public key available in environment to assist verification of his signature on clients’ digital certificate.
* **Revocation of Certificates** − At times, CA revokes the certificate issued due to some reason such as compromise of private key by user or loss of trust in the client. After revocation, CA maintains the list of all revoked certificate that is available to the environment.

Classes of Certificates

There are four typical classes of certificate −

* **Class 1** − These certificates can be easily acquired by supplying an email address.
* **Class 2** − These certificates require additional personal information to be supplied.
* **Class 3** − These certificates can only be purchased after checks have been made about the requestor’s identity.
* **Class 4** − They may be used by governments and financial organizations needing very high levels of trust.

Registration Authority (RA)

CA may use a third-party Registration Authority (RA) to perform the necessary checks on the person or company requesting the certificate to confirm their identity. The RA may appear to the client as a CA, but they do not actually sign the certificate that is issued.

Certificate Management System (CMS)

It is the management system through which certificates are published, temporarily or permanently suspended, renewed, or revoked. Certificate management systems do not normally delete certificates because it may be necessary to prove their status at a point in time, perhaps for legal reasons. A CA along with associated RA runs certificate management systems to be able to track their responsibilities and liabilities.

Private Key Tokens

While the public key of a client is stored on the certificate, the associated secret private key can be stored on the key owner’s computer. This method is generally not adopted. If an attacker gains access to the computer, he can easily gain access to private key. For this reason, a private key is stored on secure removable storage token access to which is protected through a password.

Different vendors often use different and sometimes proprietary storage formats for storing keys. For example, Entrust uses the proprietary .epf format, while Verisign, GlobalSign, and Baltimore use the standard .p12 format.

Hierarchy of CA

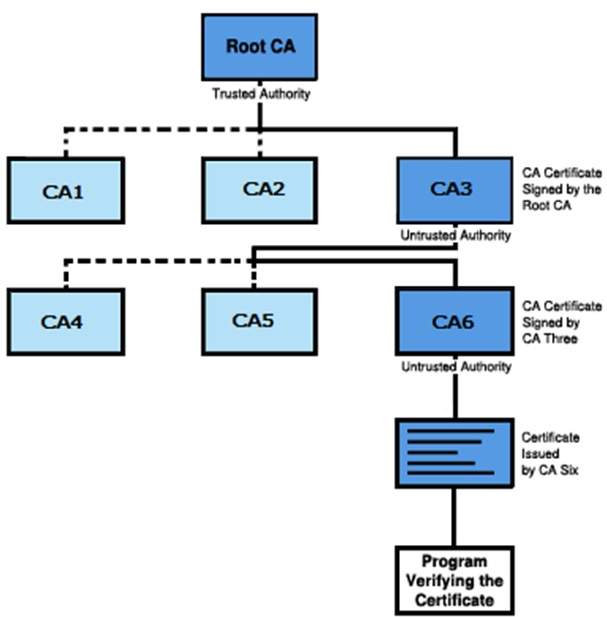
With vast networks and requirements of global communications, it is practically not feasible to have only one trusted CA from whom all users obtain their certificates. Secondly, availability of only one CA may lead to difficulties if CA is compromised.

In such case, the hierarchical certification model is of interest since it allows public key certificates to be used in environments where two communicating parties do not have trust relationships with the same CA.

* The root CA is at the top of the CA hierarchy and the root CA's certificate is a self-signed certificate.
* The CAs, which are directly subordinate to the root CA (For example, CA1 and CA2) have CA certificates that are signed by the root CA.
* The CAs under the subordinate CAs in the hierarchy (For example, CA5 and CA6) have their CA certificates signed by the higher-level subordinate CAs.

Certificate authority (CA) hierarchies are reflected in certificate chains. A certificate chain traces a path of certificates from a branch in the hierarchy to the root of the hierarchy.

The following illustration shows a CA hierarchy with a certificate chain leading from an entity certificate through two subordinate CA certificates (CA6 and CA3) to the CA certificate for the root CA.

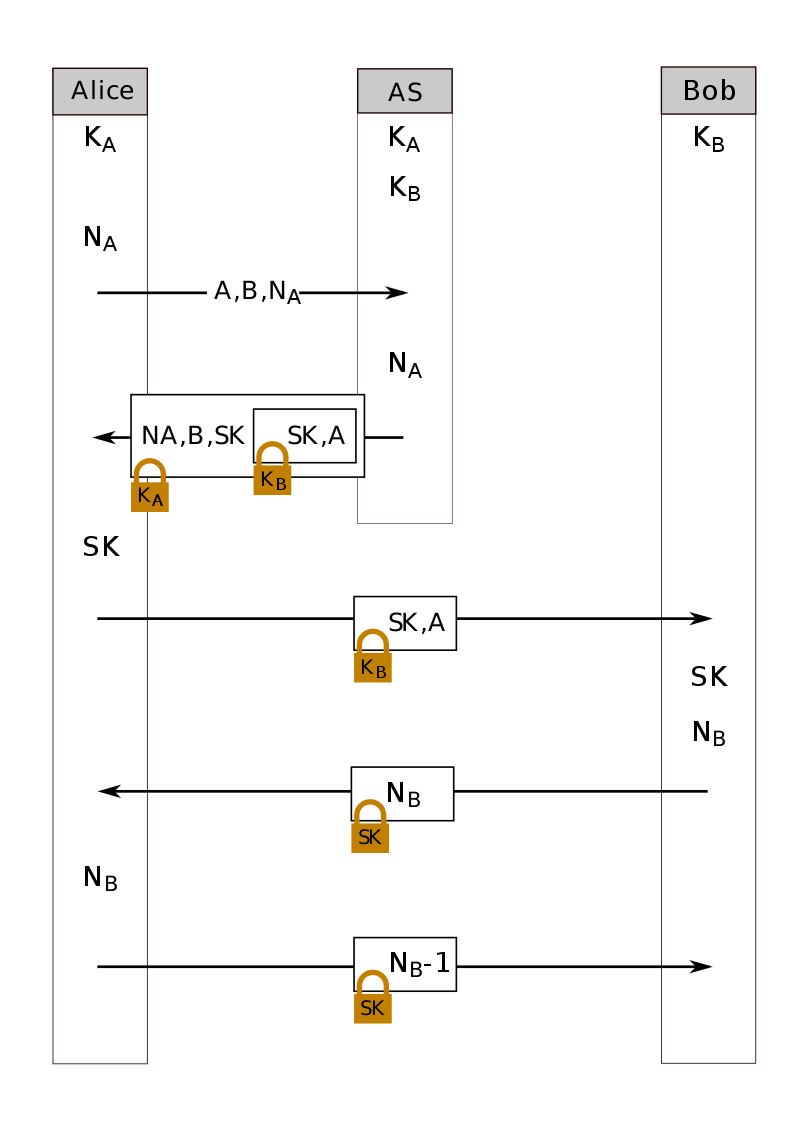


Verifying a certificate chain is the process of ensuring that a specific certificate chain is valid, correctly signed, and trustworthy. The following procedure verifies a certificate chain, beginning with the certificate that is presented for authentication −

* A client whose authenticity is being verified supplies his certificate, generally along with the chain of certificates up to Root CA.
* Verifier takes the certificate and validates by using public key of issuer. The issuer’s public key is found in the issuer’s certificate which is in the chain next to client’s certificate.
* Now if the higher CA who has signed the issuer’s certificate, is trusted by the verifier, verification is successful and stops here.
* Else, the issuer's certificate is verified in a similar manner as done for client in above steps. This process continues till either trusted CA is found in between or else it continues till Root CA.

1. Same as 40

The **Needham–Schroeder protocol** is one of the two key transport protocols intended for use over an insecure network, both proposed by [Roger Needham](https://en.wikipedia.org/wiki/Roger_Needham) and [Michael Schroeder](https://en.wikipedia.org/wiki/Michael_Schroeder).[[1]](https://en.wikipedia.org/wiki/Needham%E2%80%93Schroeder_protocol#cite_note-needham-schroeder-1) These are:

* The *Needham–Schroeder Symmetric Key Protocol*, based on a [symmetric encryption algorithm](https://en.wikipedia.org/wiki/Symmetric-key_algorithm). It forms the basis for the [Kerberos](https://en.wikipedia.org/wiki/Kerberos_(protocol)) protocol. This protocol aims to establish a [session key](https://en.wikipedia.org/wiki/Session_key) between two parties on a network, typically to protect further communication.
* The *Needham–Schroeder Public-Key Protocol*, based on [public-key cryptography](https://en.wikipedia.org/wiki/Public-key_cryptography). This protocol is intended to provide mutual [authentication](https://en.wikipedia.org/wiki/Authentication) between two parties communicating on a network, but in its proposed form is insecure. 

1. https://searchnetworking.techtarget.com/definition/virtual-private-network