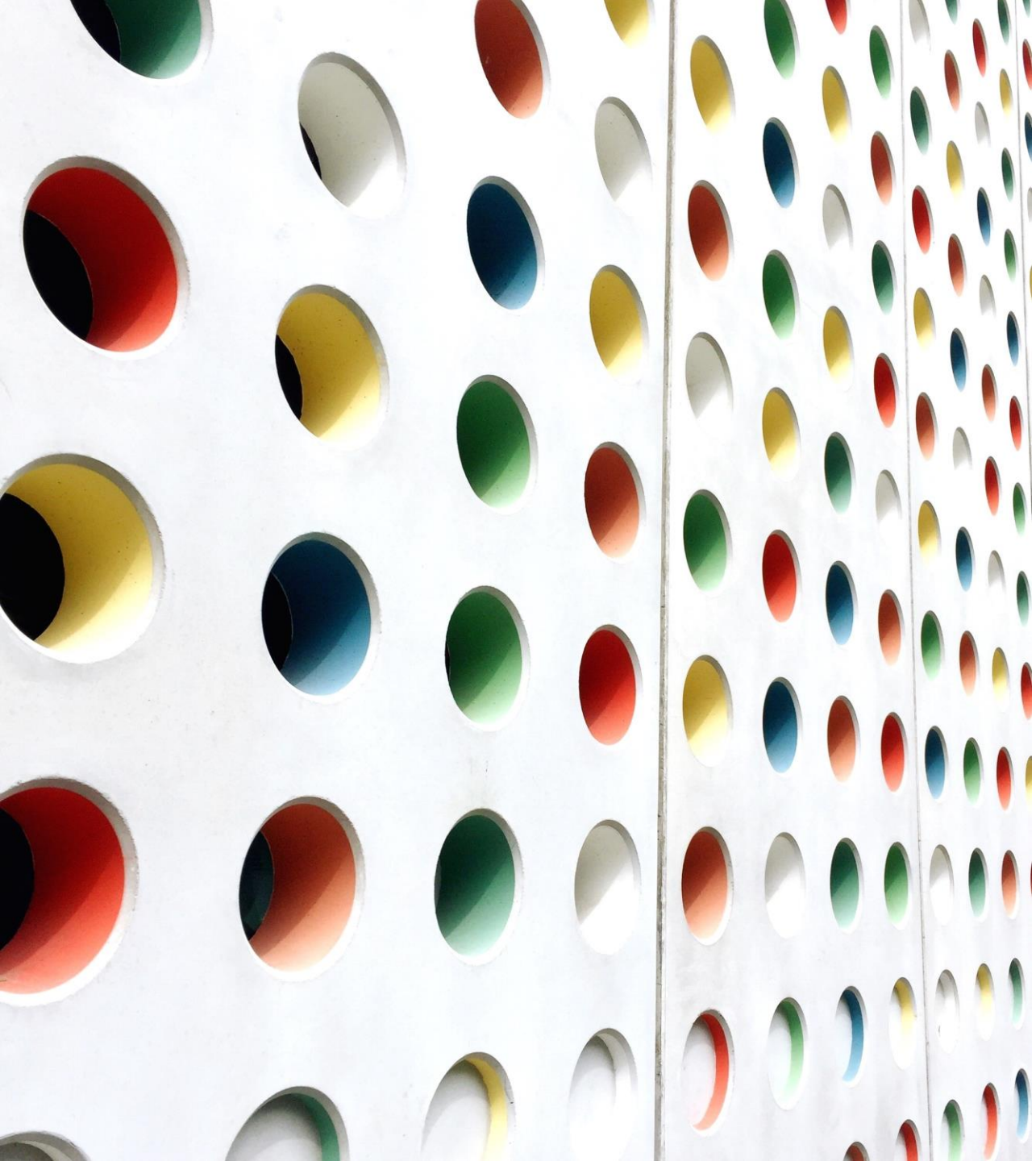


X.509 Certificate

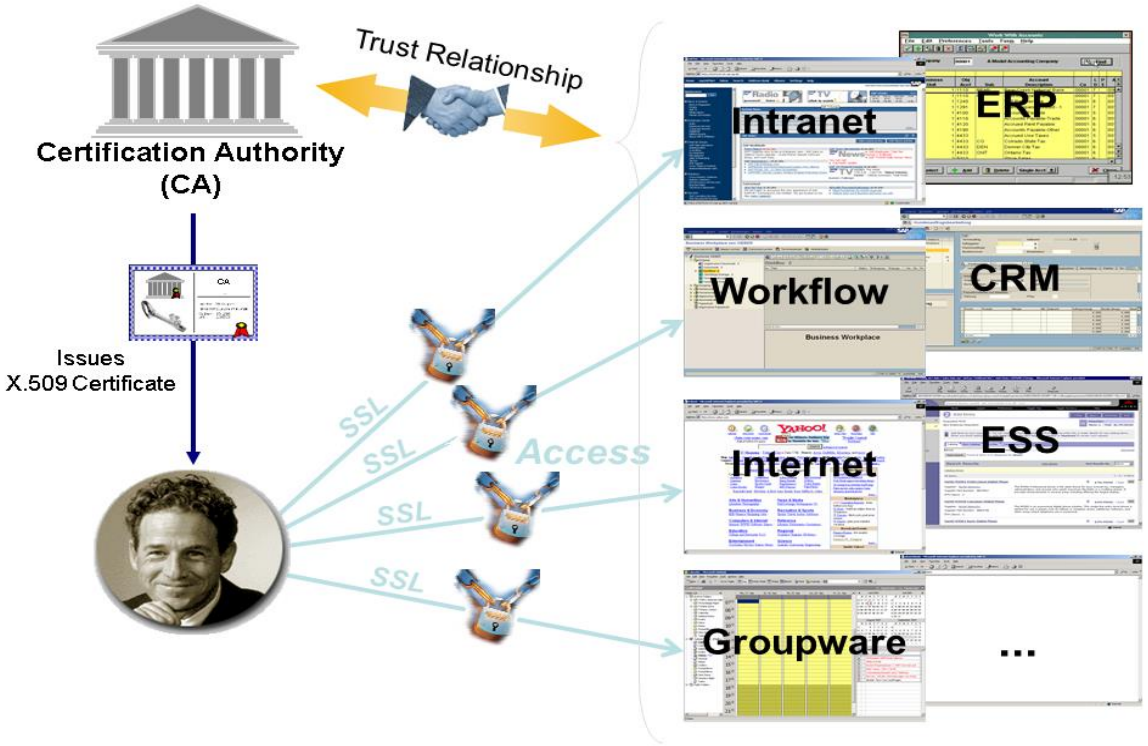
WHAT IS X.509...????

- X.509 is a certificate provided to individuals, organizations, and devices that need to securely communicate over networks, particularly on the internet.
- It is an alternative for authenticating with a user ID and passwords, users can present X.509 client certificates for accessing Web applications. In this case, user authentication takes place using the underlying Secure Sockets Layer (SSL) protocol and users do not need to interactively enter a password for logon.
- They play a crucial role in establishing trust and ensuring the Confidentiality, Integrity and Authenticity of data exchanged over the internet.

WHO will provide this X.509

CERTIFICATION AUTHORITY:

- *CA(Certificate Authority) is a trusted entity that issues digital certificates to organizations or individuals after verifying their identity.*
- *Certificate Authorities can be commercial entities, government agencies, or non-profit organizations.*



WHO CAN GET THIS CERTIFICATE..??

Some common examples of entities that may be issued X.509 certificates :

1. *Websites and Web Servers:* - Websites and web servers use X.509 certificates to prove their identity to visitors' web browsers.

2. *Email Servers and Clients:* - Email servers and clients use X.509 certificates to enable secure email communication via protocols like SMTP (Simple Mail Transfer Protocol) and IMAP (Internet Message Access Protocol).

3. *Individual Users:* - Individual users may also be issued X.509 certificates for various purposes, such as digital signatures, secure email communication (S/MIME), client authentication. Using x.509, clients digital signature is verified.

SIGNATURE GENERATION

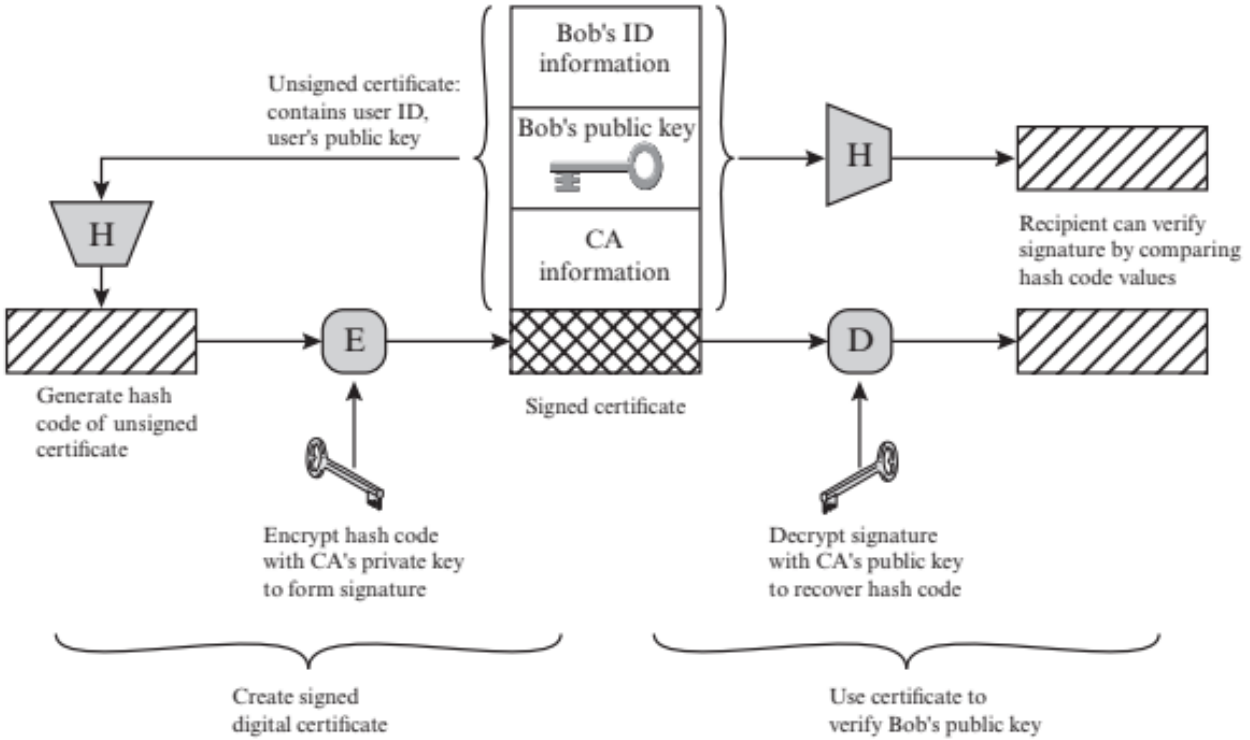


Figure 14.14 X.509 Public-Key Certificate Use

X.509 CERTIFICATE FORMAT

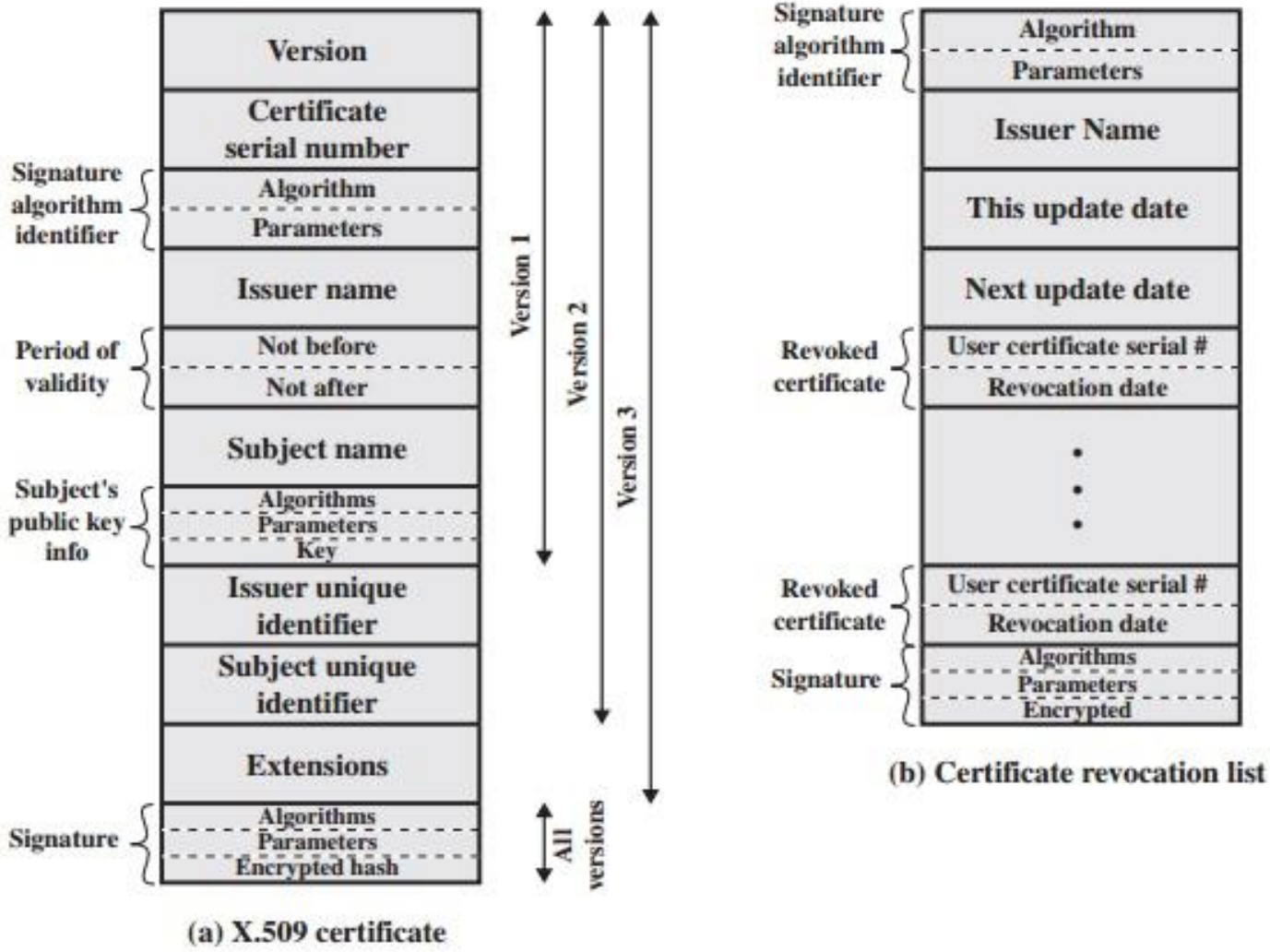


Figure 14.14 X.509 Formats

- **Version**: Indicates the format of the certificate. Version 1 is the default, but if the certificate includes unique identifiers for issuer or subject, it's version 2. If extensions are present, it's version 3.
- **Serial number**: A unique integer assigned by the Certificate Authority (CA) to this certificate.
- **Signature algorithm identifier**: Specifies the algorithm used to sign the certificate. Not very useful since this information is also included in the signature field.
- **Issuer name**: The name of the CA that issued and signed the certificate.
- **Validity period**: The duration during which the certificate is considered valid, specified by its start and end dates.

- **Subject name**: The name of the entity (user) to whom the certificate is issued. It certifies the public key belonging to this entity.
- **Subject's public-key information**: Includes the public key of the subject along with the algorithm identifier and any associated parameters for using the key.
- **Issuer unique identifier**: An optional field used to uniquely identify the issuing CA, especially if the X.500 name has been reused.
- **Subject unique identifier**: An optional field used to uniquely identify the subject, especially if the X.500 name has been reused.
- **Extensions**: Added in version 3, extensions provide additional information or capabilities beyond the basic fields of the certificate.
- **Signature**: This field covers all other fields of the certificate and includes the digital signature applied to the certificate. It also contains the algorithm identifier for the signature.


THANK YOU!