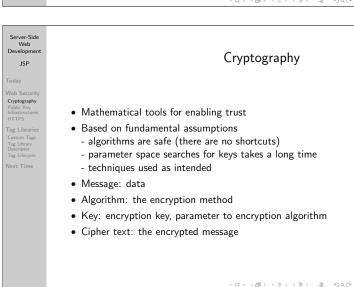
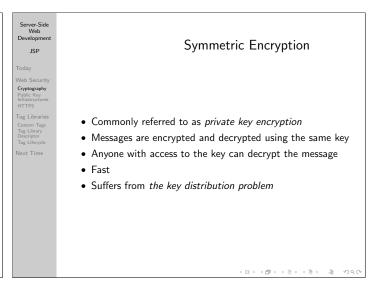
Server-Side Web Development
JSP
Today
Web Security Cryptography Public Key Infrastructures HTTPS
Tag Libraries Custom Tags Tag Library Descriptor
Tag Lifecycle Next Time



Server-Side Web Development JSP	Web Security						
Today							
Web Security Cryptography Cryptography Fig. 10 April 1997 Cryptography Tag Libraries Custom Tags Tag Library Descriptor Tag Lifecycle Next Time	 Based on cryptography SSL / TLS current encryption standards HTTPS = HTTP through a SSL tunnel (no changes in JSP required) 						



Server-Side Web Development JSP Today Web Security Cryptography	One-Way Encryption
Public Key Infrastructures HTTPS Tag Libraries Custom Tags Tag Library Descriptor Tag Lifecycle Next Time	 Messages are encrypted using secret keys Messages can not be decrypted Cipher texts are (to a high probability) uniquely mapped to message content Cipher texts are used instead of messages in situations where messages must be kept secret (e.g., passwords) Closely related to hashcodes and Message Authentication Codes (MACs)



Server-Side Web Development JSP

Web Security
Cryptography
Public Key
Infrastructures

Tag Libraries
Custom Tags
Tag Library
Descriptor
Tag Lifecycle
Next Time

Asymmetric Encryption

- Commonly referred to as public key encryption
- Messages are encrypted using key pairs (public & private)
- One key used for encryption, the other for decryption
- Public key distributed as much as possible
- Private key kept secret
- Versatile and more secure than symmetric algorithms
- Slow

ロ ト 4 回 ト 4 ミ ト 4 ミ ト 9 Q

Server-Side Web Developmen

JSP

Web Security
Cryptography
Public Key
Infrastructures

Tag Libraries Custom Tags Tag Library Descriptor Tag Lifecycle

Asymmetric Encryption

- Encrypt message using public key encryption
- Encrypt message using private key signatures
- Messages can be both encrypted and signed
- As long as the keys can be trusted
 - messages can be kept secret (only receiver can decrypt)
 - senders and receivers can be authenticated
 - message content can be trusted

Server-Side Web Development JSP

Web Security Cryptography Public Key Infrastructures HTTPS

Tag Library Descriptor Tag Lifecycle Next Time

Certificates

- Certificate = signed tuple of public key & identity
- Certificates can be self-signed or signed by others
- Self-signed certificates can be used for encryption (but suffer from *the key distribution problem*)
- Certificates signed by trusted parties can be used for encryption, authentication and message integrity checks

ㅁ > (중) + (원 > (원 > 원 -) 역(

Server-Side Web

JSP Today

Cryptography
Public Key
Infrastructures

Tag Librarie Custom Tags Tag Library Descriptor Tag Lifecycle

Public Key Infrastructures (PKI)

- Virtual infrastructures consisting of clients, servers and Certificate Authorities (CA)
- CAs are trusted third parties which provide signed certificates (i.e., signs public keys)
- CA certificates are distributed in browsers and similar tools (trusted and considered known by all)
- Since CA public keys are known, (signed) certificates can be validated offline (without connecting to the CA)
- Secure connections are established between parties using certificates and encryption algorithms
- Network traffic tunneled through encrypted channels

4 B > 4 B > 4 B > - 토 - 9 Q @

Server-Side Web Pevelopment JSP

Today
Web Securit
Cryptography
Public Key

Tag Libraries Custom Tags Tag Library Descriptor Tag Lifecycle Next Time

Secure Socket Layer (SSL)

- A protocol for establishing secure connections using certificates and cryptography algorithms
- $\bullet \ \, \text{Transport Level Security (TLS)} = \text{SSL v3.0 (almost)}$
- Clients use server certificate to authenticate server
- Servers use client certificate to authenticate client (optional)
- Once identities have been established, encryption keys are exchanged and symmetric encryption algorithms are used
- SSL clients uses keystores to manage certificates and keys

(ロ) (部) (き) (き) モーカス(C)

Server-Side Web Developmen

dav

Web Security Cryptography Public Key Infrastructures

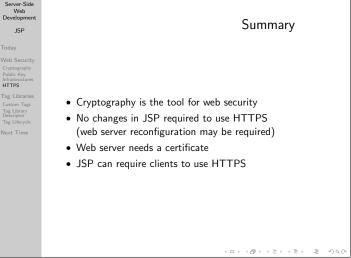
Tag Librarie Custom Tags Tag Library Descriptor Tag Lifecycle

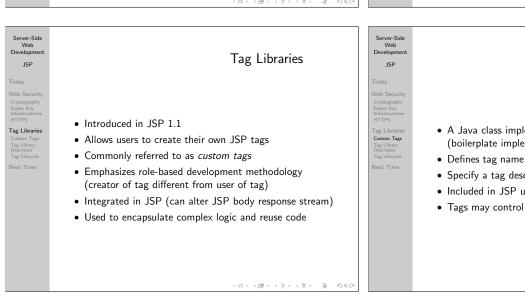
Keystores

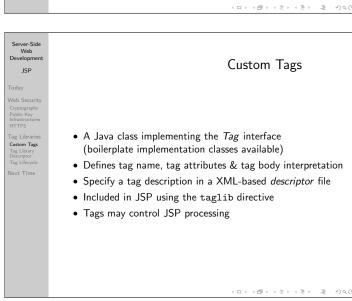
- $\bullet\,$ An encrypted database used to store keys and certificates
- Usually stored in a single file called .keystore
- Applications must provide database decryption key (username & password) to access keystore content
- Keystores only containing public keys and certificates are commonly referred to as truststores
- Keystores can be shared between SSL applications (usually only done for truststores)

4 D > 4 B > 4 E > 4 E > B 9 Q C

Not an actual protocol **One of the server needs to be provided with a certificate **Interest Time **Interest Time** **Not an actual protocol **HTTPS = HTTP through a SSL/TLS tunnel **The server needs to be provided with a certificate **If the server is to authenticate clients, the clients need (CA signed) certificates as well **HTTPS Web servers usually references keystores via configuration (providing filename, username, password) **Default port 443 (HTTP default port is 80) **JSP can check if a page was requested via HTTPS using request.isSecure() **HTTPS / SSL is considered safe (today)







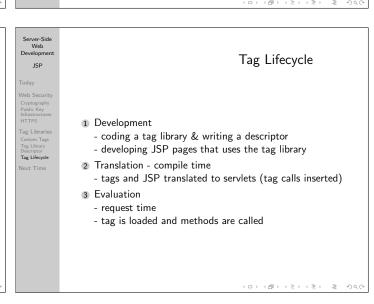
```
Server-Side
Web Development
JSP

Today
Web Security
Crystegraphy Public Key
Infratructures
HTTPS

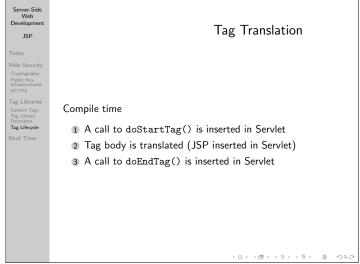
Tag Libraries
Custom Tags
Tag Libraries
Tag Set Parent ();
void set Parent (Tag t);
void set Page Context (Page Context pc);
void release ();
int do End Tag ();
int do Start Tag ();
}
```


Server-Side Web Development JSP Today Web Security Cryptography Public Key Infrastructures HTTPS Tag Libraries Custon Tags The Library The Library Descriptor **ML-based configuration file** Provides a mapping from tag names to tag Java classes Tag Library Infrastructures Provides a mapping from tag names to tag Java classes Contains tag library information and tag descriptions Tag descriptions direct how the tag is utilized (by the JSP engine, include tag body etc) Required, one per tag library

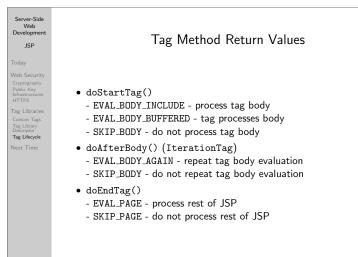
Descriptor Content JSP • name - tag alias for use in JSP (coupled to tag library namespace) · tagclass - fully qualified implementation class name Tag Librar • attribute - tag attributes (optional) Tag Library Descriptor (used as tag parameters, values delivered as Strings) - name - attribute name - required - attribute required to process tag flag - rtexprvalue - attribute value from JSP expression flag • info - descriptive information about tag (optional) body-content - tag body processing directives (optional) - EMPTY - no tag body - JSP - body contains JSP - TAGDEPENDENT - tag processes body itself



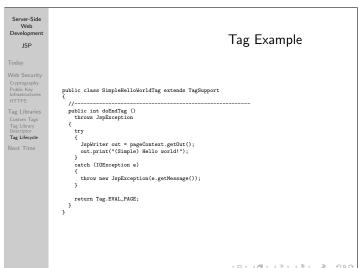


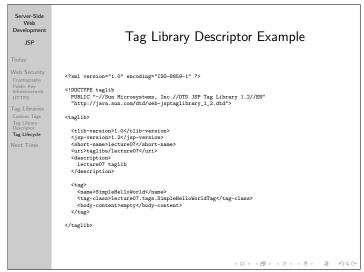


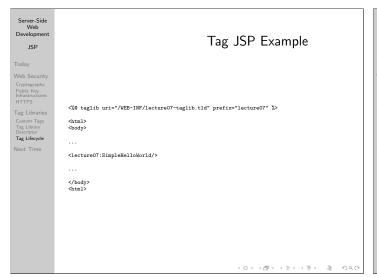
Today Web Security Crystography Public Reg Clusten Tags Tag Libraries Tag Libraries Tag Libraries Tag Library Tag Lifercyte Next Time Request time 1 setPageContext() called, page context provided 2 setParent() called, page hierarchy established (used for nested tags) 3 setAttribute() is called for attributes 4 doStartTag() called, return value directs processing 5 Tag body processed (if so instructed by doStartTag()) 6 doEndTag() is invoked, return value directs processing 7 release() is called to release tag resources (so that tag objects can be reused by thread pools)

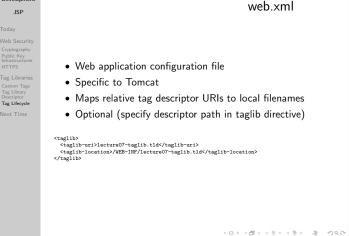


(D) (B) (E) (E) E 990









Server-Side Web Development JSP	Summary	Server-Side Web Development JSP		Next Time
Today Web Security Cryptography Public Key Infrastructure HTTPS Tag Libraries Custom Tags Tag Library Descriptor Tag Lifecyte Next Time	 Tab libraries are used to extend the JSP tag set Very powerful way to reuse Java code in JSP Custom tags can be used as any JSP tag Tag behavior determined by tag developer Custom tags well suited to hide large logic segments Custom tags are never visible to web clients 	Today Web Security Cryptography Public Key Infrastructures HTTPS Tag Libraries Custom Tags Tag Library Descriptor Tag Lifecycle Next Time	Web Services	10>(B)(E)(E) & v2)Q(