PKI – créer une identité serveur Utilisation de l'assistant

CREATE A SERVER IDENTITY	
IDENTITY OPTIONS - CREATION WIZAR	D
Fully Qualified Domain Name (FQDN):	server1.training.net
ID:	server1.training.net
	X CANCEL

PKI – créer une identité serveur

- Utilisation de l'assistant
 - nom FQDN > inscrit dans le certificat
 - Doit coïncider avec le nom DNS

PKI – créer une identité serveur

EATE A SERVER IDENTITY	1774 DD	
DENTITY OPTIONS - CREATION V		
Select the parent Autority		
Parent CA:	Root-Ca-Training	* X
CA passphrase:	******	P
Autority attributes	Training	
Organizational unit:	CSNE	
City (L):	Paris	
State (ST):	ldf	
Country:	France	•
	Y CANCEL & DDI	EVIOUS NEXT

BTS SIO

PKI – créer une identité serveur

- Mot de passe du CA requis
 - Accès à la clé privé du CA
 - Signature du certificat serveur

PKI – créer une identité serveur

CREATE A SERVER IDENTITY		
IDENTITY OPTIONS - CREAT	ION WIZARD	
		RSA
		SECP
Validity (days):	365	BRAINPOOL
Type de clé:	BRAINPOOL	-
Key size (bits):	512	*
	× CAN	CEL « PREVIOUS » NEXT

BTS SIO

PKI – créer une identité serveur

- Préciser :
 - La durée de validité du certificat
 - La taille de la clé de chiffrement

Bloc 3 PKI – créer une identité serveur

Certificate			2
General Details Certification Path			
Show: <all></all>		~	
Field Authority Ke Basic Constr Enhanced Ke Certificate P	ey Identifier aints ey Usage olicies	Value KeyID=e551c3ca6c85a7e2adf. Subject Type=End Entity, Pat Server Authentication (1.3.6 [1]Certificate Policy:Policy Ide	^
Subject Alter	rnative Name	DNS Name=alias-server1.train	
Key Usage		Digital Signature, Key Encipher. d6ea5db78193dec9da3613a6f.	•
DNS Name=alias	-server1.training.ne ki-adm@training.ne	t	
	General Details Show: <all> Field Authority Ke Basic Constr Basic Constr Certificate P Subject Alter Key Usage Thumbprint DNS Name =alias RFC822 Name =p</all>	General Details Certification Path Show: <all> Field Authority Key Identifier Basic Constraints Enhanced Key Usage Certificate Policies Subject Alternative Name Key Usage Thumbprint DNS Name =alias-server 1. training.ne RFC822 Name =pki-adm@training.ne</all>	Certificate General Details Certification Path Show: <all> Field Value Muthority Key Identifier KeyID=e551c3ca6c85a7e2adf Basic Constraints Subject Type=End Entity, Pat Enhanced Key Usage Server Authentication (1.3.6) Subject Alternative Name DNS Name=alias-server 1.train Key Usage Digital Signature, Key Encipher Thumbprint d6ea5db78193dec9da3613a6f</all>

PKI – créer une identité serveur

• Ajout possible

– D'autres noms DNS