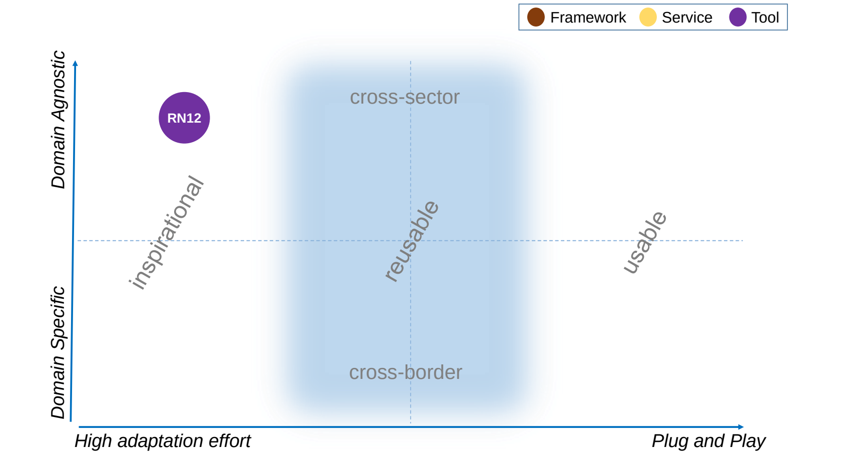
[RN12] Digital Certificates (X.509 standard)

Digital Certificates (X.509 standard)	
Summary	
ID	RN12
Initiative	ECRN
Short description	Each user of ECRN Service owns two digital certificates of different typologies: - The “authentication certificate” is used for recognizing the suer when accesses the web application. This identification allows checking the user’s right to use the application and to retrieve the connected role to control which specific functions he/she can use and which data he/she can look at. - The “signature certificate” is used by the user to digitally sign the documents he/she manages. Thanks to this signature, the ECRN platform guarantees the security of the documents (protection and integrity) and the security of their origin, in terms of who has signed and sent the document (non-repudiability). Both the typology of a digital certificates are allocated on the same physical support that can be a smartcard or a USB token. The first one requires a smartcard reader connected to a PC USB port and the second one can be directly inserted in a PC USB port.
Owner	Consortium: http://www.ecrn.eu/BBB/index.php?option=com_content&view=article&id=45&Itemid=55&lang=en
Contact	kjell.hansteen@ec.europa.eu
Type	Tool
Sub-Type	Component
IPR	Not Available/Not Found
Status	Operational
More details	
Aggregated business need	ABN – 5 Need for mechanisms to ensure secure data exchange
Documentation	ECRN D43 ECRN Web Application - Functional and Technical specifications(1).pdf
EIRA	
View	Technical View - Infrastructure
Building Block	Trust Service Provisioning Component
Reusability	

Landscape


● Framework
● Service
● Tool
Domain Agnostic
Domain Specific
RN12
cross-sector
inspirational
reusable
usable
cross-border
High adaptation effort
Plug and Play