9. Übungsaufgabe: Gültigkeitsmodelle

Die für die Bearbeitung der Aufgabe wesentlichen Daten der verwendeten Zertifikate sind nachfolgend dargestellt. Alle Signaturen sind gültig, sie sind tatsächlich von dem Aussteller eines Zertifikats vorgenommen wurden. Es sind keine Zertifikate revoziert.

Certificate A	
Serial Number	4711
Issuer	RootCA
NotBefore	1.1.2019
NotAfter	31.5.2021
Subject	RootCA
Public Key	key-0x0815
SignedBy	RootCA with key-0x0815

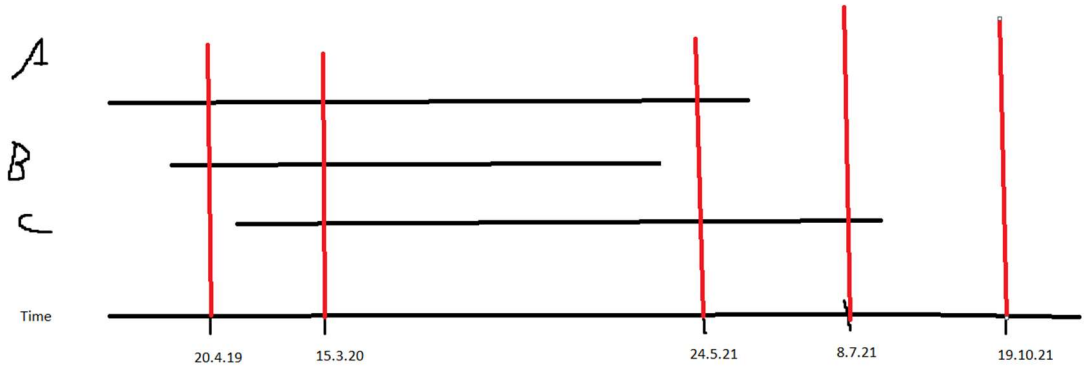
Certificate B	
Serial Number	4712
Issuer	RootCA
NotBefore	1.3.2019
NotAfter	31.3.2021
Subject	SubCA
Public Key	key-0xFEED
SignedBy	RootCA with key-0x0815

Certificate C	
Serial Number	280815
Issuer	SubCA
NotBefore	1.5.2019
NotAfter	31.7.2021
Subject	Alice
Public Key	key-0xAABB
SignedBy	SubCA with key-0xFEED

Alice signiert ein Dokument an den folgenden Zeitpunkten:

- 20.4.2019
- 15.3.2020
- 24.5.2021
- 8.7.2021
- 19.10.2021

a) Erstellen Sie eine Abbildung mit der Zeitachse, den Gültigkeitszeiträumen der Zertifikate und den Signaturzeitpunkten.



b) In der folgenden Tabelle tragen Sie das Ergebnis der Verifikation am 1.1.2021 ein. Mögliche Werte sind „gültig“ oder „ungültig“.

Signatur-Zeitpunkt	Schalenmodell	Modifiziertes Schalenmodell	Kettenmodell
20.4.2019	gültig	n gültig	n gültig
15.3.2020	gültig	gültig	gültig

c) In der folgenden Tabelle tragen Sie das Ergebnis der Verifikation am 1.1.2022 ein. Mögliche Werte sind „gültig“ oder „ungültig“.

Signatur-zeitpunkt	Schalenmodell	Modifiziertes Schalenmodell	Kettenmodell
20.4.2019	n gültig	n gültig	n gültig
15.3.2020	n gültig	gültig	gültig
24.5.2021	n gültig	n gültig	gültig
8.7.2021	n gültig	n gültig	gültig
19.10.2021	n gültig	n gültig	n gültig

d) Geben Sie für alle Modelle die jeweiligen Zeiträume an, in denen Alice eine gültige Signatur erstellen kann.

Signierzeitraum	Schalenmodell	Modif. Schalenmodell	Kettenmodell
Von	-	1.5.2019	1.5.2019
Bis	-	31.3.2021	31.7.2021

PS: Beim Schalenmodell hängt es vom Prüfungszeitraum abs