CHAPTER 4

USER-DEVICE AUTHENTICATION MODEL DESIGN

4.1 Overview

This chapter presents the User-Device Authentication Model using Digital Certificate for Smartphone users which includes the proposed User-Device Authentication Model implementing Digital Certificate for Smartphone User as well as the diagrams related to the proposed model. These diagrams include the Unified Modelling Language (UML) such as Flowchart Diagrams.

4.2 Flowchart Diagram

Flowchart represents the workflow or the process of the authentication model where it shows step-through various types of boxes. Figure 4.1 below shows the flowchart of the User-Device Authentication Model with Digital Certificate for Smartphone User.

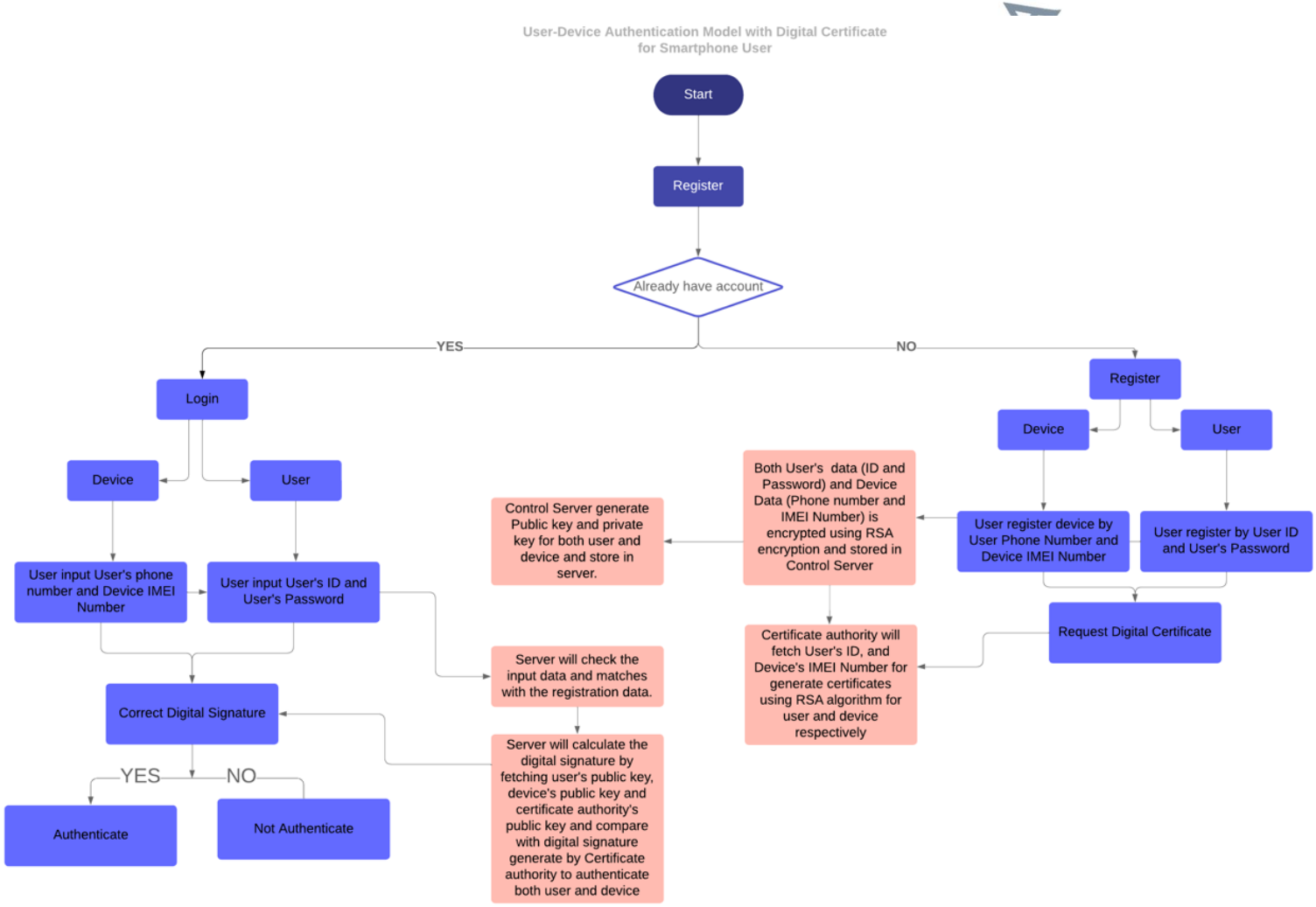

Figure 4. 1: Flowchart of the User-Device Authentication Model with Digital Certificate for Smartphone User

4.2.1 Explanation of the Flowchart

Based on the flowchart shown in Figure 4.1, the process flow of the User Device Authentication Model with digital certificates for smartphone users commences with the required registration of both the user and the device. The user will be asked to furnish their user ID and password while the device is required to register their phone number and IMEI number. Subsequently, the registered information is stored in the control server. The control server then generates the public and private keys for the user and device respectively, which are securely preserved within its confines. The public key and private key generated for both user and devise are used to encrypt the user's ID and device's IMEI number using RSA encryption. Once the user's ID and device's IMEI number are encrypted, the encrypted date is stored in the control server. After the user and device complete the registration process, they proceed to individually request their Digital Certificates. The creation of these digital certificates requires the involvement of a third-party user, with the Certificate Authority being entrusted with this responsibility. The Certificate Authority certification authority retrieves the necessary information from the control server to facilitate the creation of the digital certificates. The digital certificate is generated by signing the user's ID and device IMEI's number using RSA digital signature algorithm.

After the digital certificates have been successfully created and stored by the certification authority, the subsequent login process requires sequential authentication of the user and the device. The user will be asked to enter their user ID and password while the device will require them to enter their phone number and IMEI number. Authentication calculations are performed in which the user and the device are verified by comparing their public keys and digital signatures acquired from the control server and the certificate authority. The prerequisite for successful login of the user and device

is joint authentication. A further explanation of these processes is provided in detail in the subsequent subtopic 4.3.

4.3 User-Device Authentication Model with Digital Certificate for Smartphone User

This subchapter presents the flow of the User-Device Authentication Model with Digital Certificate for Smartphone as depicted in Figure 4.2 until 4.4 below. There are three phases of this proposed model, which are the Registration Phase, Digital Certificate Issue Phase, and Authentication/Verification Phase. Each phase correlates to the other phase to authenticate the user.

4.3.1 Phase 1: Registration Phase

The process flow of the proposed Authentication Model for Phase 1, or the registration phase, is shown in Figure 4.2 below. In this stage, users register by entering their User Identity, U_{id}, and setting a password, U_{pw} that corresponds to it. The U_{id} and U_{pw} are then safely kept inside the control server (CS). In addition, users proceed to register their device by obtaining the International Mobile Equipment Identity (IMEI) number (D_{in}) from the device itself and entering their phone number (U_{pn}). The control server (CS) then stores these identifiers (U_{pn} and D_{in}). The Control Server (CS) utilizes a designated random number generator to generate two large prime numbers, p, and q, at random to begin computing the user's cryptographic key. This is a noteworthy approach. The value *n* is calculated by multiplying both p and q as shown in equation 4.1 below.

$$n = p \,.\, q$$

(Equation 4. 1): Value of n

Once the value *n* is obtained, the next step is to calculate the Euler's Totient with the formula shown in equation 4.2 below.

$$\Phi(n) \;=\; (p-1)(q-1)$$

(Equation 4. 2): Euler's Totient

The equation Euler's Totient above is used to calculate the public exponential, e. Public exponential, e, is selected by e ∈ {1,2, . . . , Φ(n)−1} such that gcd(e,Φ(n)) = 1. The private key d is calculated based on equation 4.3 below.

$$d \;\cdot e \;\equiv\; 1 \; mod \Phi(n)$$

(Equation 4. 3): Private Key, d.

The private key user is depicted as Kpr(u) = d. Once the user has obtained the private key, the public key of the user is calculated using the equation 4.4 below.

$$Kpub(u) \;=\; (n, e)$$

(Equation 4. 4): public key of User.

The procedure is repeated to obtain the Public Key and Private Key for the device, which are represented as Kpub(d) and Kpr(d), respectively. ASCII encoding is used to convert the Uid and Din into their respective ASCII values. After that, the value is encrypted using the User's Public Key, Kpub(u), along with the Uid and the Device's Public Key, Kpub(d), for Din.

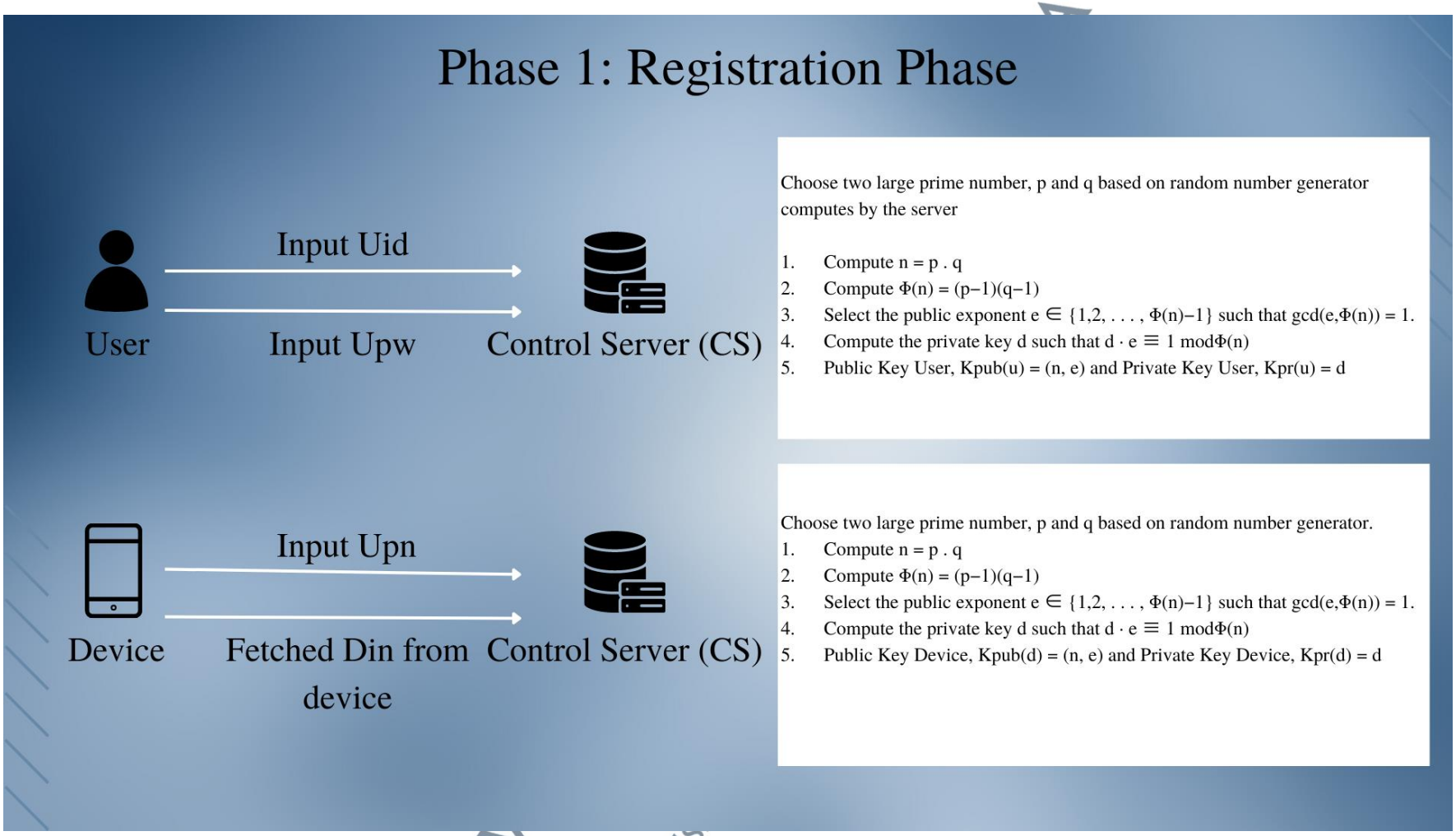

Figure 4. 2: Phase 1: Registration Phase

4.3.2 Phase 2: Digital Certificate Issue Phase

The process flow of the proposed Authentication Model for Phase 2, with a particular emphasis on the digital certificate issuance phase, is shown in Figure 4.3 below. In this stage, users have to request digital certificates for their devices and themselves. The control server (CS) provides the Certificate Authority (CA), which is in charge of issuing these certificates, with the user's public key (Kpub(u)), user ID (U_{id}), and device IMEI number (D_{in}) as shown in equation 4.5 below.

$$Sa(U) = sigKpr(ca), CA(kpub(u), Uid, Din$$

(Equation 4. 5): Digital Signature of User.

The CA then signs the certificate with its private key (Kpr(ca)), which includes the user's public key, user ID, and device IMEI number. The CA keeps the user's certificate after it is issued with the information as shown in equation 4.6 below.

$$CertU = [(kpub(u), Uid, Din), Sa(U)]$$

(Equation 4. 6): Digital Certificate of User.

The information in the certificate of the users is as user's public key which includes the user's ID (Uid) and the Device's IMEI number (D_{in}), as well as the Signature of the digital certificate, The steps below are repeated to obtain the digital certificate for the device. Once both of the certificates are created, both the user and their device receive a notification verifying the successful creation of the certificate. Each year, these certificates must be renewed to preserve the security of the user's key. The process is reiterated to procure a certificate for the user's device, with the CA signing information within the device's certificate, including the device's public key (Kpub(d)), device IMEI number, and user ID, using its private key (Kpr(ca)).

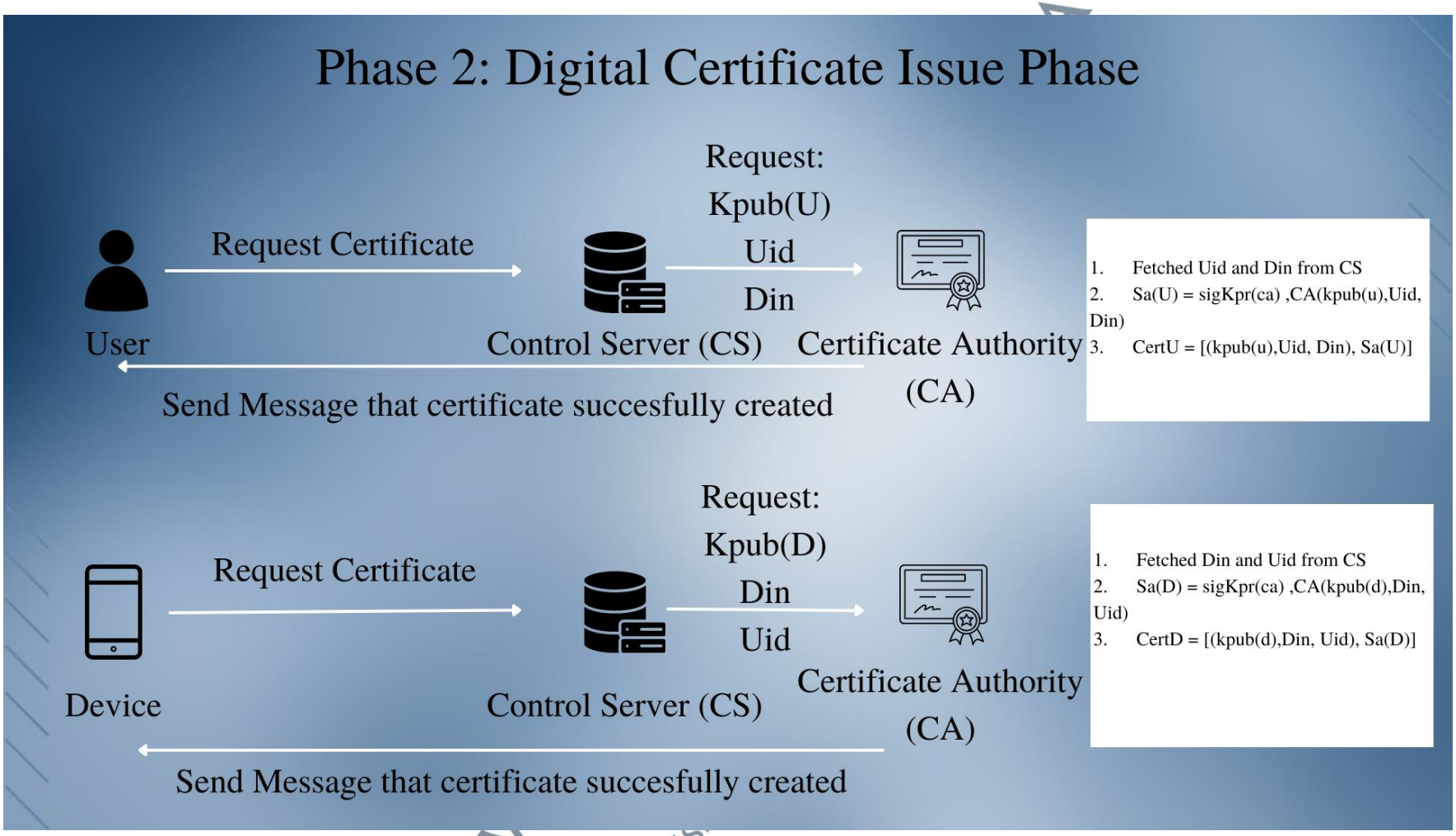

Figure 4. 3: Phase 2: Digital Certificate Issue Phase

4.3.3 Phase 3: Authentication/Verification Phase

Phase 3, or the authentication/verification stage, is represented by the progression of the proposed Authentication Model in Figure 4.4. The user must enter their UserID, (Uid), password (Upw), and device's phone number (Upn)in this phase, which expands on Phases 1 and 2. The IMEI number of the device, Din is also obtained. If the user enters Uid, Upw, or Upn incorrectly, an error message asks them to enter the correct information. The Control Server (CS) performs an authentication calculation to confirm the user's signature after receiving accurate input. This entails obtaining the Certificate Authority (CA) (Kpub(ca)) and user (Kpub(u)) public keys from the CS. The authentication calculation uses the public key (Kpub(ca)) of the CA to compute the user's verification signature (Sa(U)') based on the provided Uid and Din (fetched from the device) as shown in equation 4.7 below.

$$Sa(U') = sigKup(ca), CA(kpub(u), Uid, Din$$

(Equation 4. 7): Verification signature of User.

The Authentication Calculation then will request the value of Sa(U) from CA and compare them with the value of Sa(U'). The user is authenticated and depicted as '1' when the Control Server compares Sa(U) with Sa(U)'. This procedure is repeated for device authentication, in which the device's details and the public key of the CA are used to compute the verification signature (Sa(D)'). Login is made possible upon successful user and device authentication whereby both are shown as '1'. It is impossible to authenticate the user and the device together if one of them is not authenticated. The suggested User-Device Authentication is described in these diagrams and protocols. This proposed model will be used for expert review validation

to verify the potential of this model to be adapted to smartphone users in the future. This expert review verification will be explained more in Chapter 5.

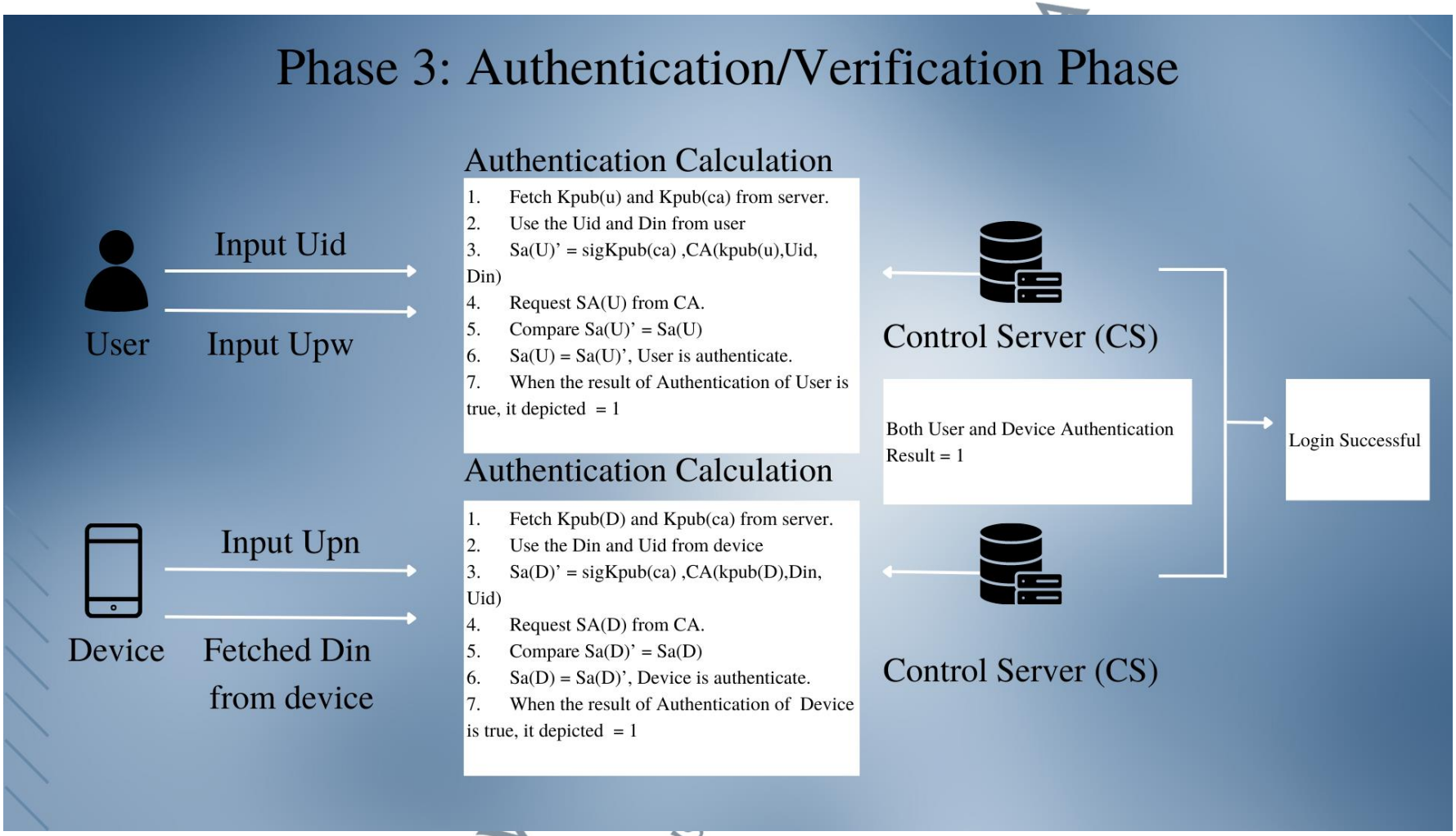

Figure 4. 4: Phase 3: Authentication/Verification Phase

4.4 Summary

This chapter presents the proposed User-Device Authentication Model with Digital Certificate for Smartphone User as well as the step-by-step process of the proposed model. There are three phases of the User-Device Authentication Model which are the registration phase, the digital certificate issue phase, and the authentication/validation phase. Moreover, although the User-Device Authentication is in the proposed model stage, presenting the Unified Modelling Language (UML) such as flowchart diagrams helps to understand the flow of the proposed model and can be used as a reference for future development of the model. This chapter also presents the development and validation process of the proposed authentication model where the authentication model is carefully developed referring to the literature review as a data source. Furthermore, the proposed authentication model is validated by presenting and answering the questionnaires related to the proposed authentication model.

The proposed model enhances the security of smartphone users in several ways compared to existing authentication methods since the proposed model authenticates both the user and their device, in contrast to many other existing models that only authenticate the user (e.g., using passwords, biometrics, or OTP). With the help of this two-factor authentication system, an attacker cannot access the user's credentials without also requiring the authenticated device such as the user’s smartphone in order to complete the login process. Because an attacker would require both the user's credentials and the actual device to assume the user's identity, this greatly lowers the risk of unauthorized access.