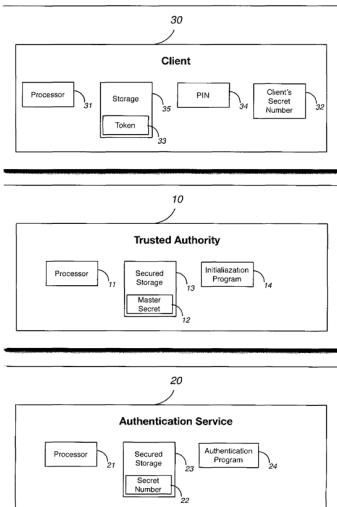
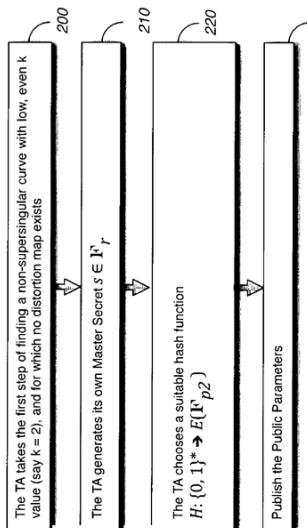
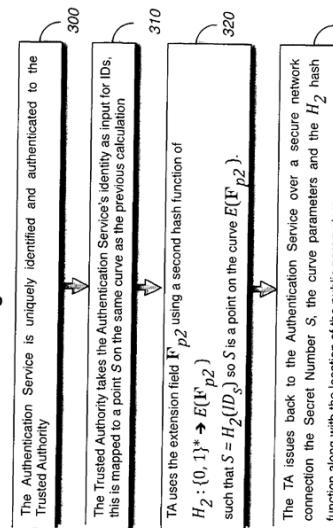


**Figure 1****Figure 4**

- 400 · The Client authenticates its identity to the Trusted Authority
- 410 · The Trusted Authority takes the Authentication Service's identity  $ID_A$  as input
- 420 · The identity is hashed and mapped to a point  $A$  of large prime order on the curve
- 430 · The Client receives from the Trusted Authority over a secure network connection  $A$  and  $S^kA$ , where  $A = c.H(ID_A)$  is a point of order  $r'$  on the base elliptic curve  $E(\mathbb{F}_p)$ .

**Figure 2****Figure 5**

- 500 · Client receives the Initialization Program
- 510 · The program takes as input the user's PIN number, and will calculate  $s\alpha A$  where  $\alpha$  is the user's PIN number
- 520 · The program then subtracts the two to get the number  $(s-\alpha)A$
- 530 · Then the program stores both  $(s-\alpha)A$  and  $A$  in the Client's browser storage
- 540 · Prompts the user to remember their PIN

**Figure 3****Figure 6**

- 600 · The Client initiates a secured connection to the Authentication Service, and the Authentication Program serves the Authentication Program to the Client
- 610 · The Authentication Program runs locally on the Client (for example, in the Client's browser) and prompts the user of the Client for their PIN and their identifier (i.e., email address)
- 620 · The Authentication Program hashes (using the same hash algorithm as the Initialization Program)  $ID_A$  and looks up the key value pair to obtain the concatenated  $(s-\alpha)A$  and  $A$  which is then used in the following section

