Specification of FSU version 1.0

NTT Secure Platform Laboratories,
NTT Corporation

March 2, 2015

1 Introduction

This document provides the specification of ID-based authenticated key exchange protocol FSU [4] that is an extension of FSU (Fujioka-Suzuki-Ustaoglu) protocol standardized in ISO/IEC 11770-3 [5].

This document uses the following notations and functions: elliptic curve parameter $\mathcal{E}$ in [1], pairing e in [2], and functions HashingToPoint, GroupMembershipTest, MGF1, ECP2OSP, OS2ECPP, FE2OSP in [3].

2 FSU system parameters

The system parameters consist of the followings.

- Let R be a point compression type specifically Compressed, Uncompressed or Hybird.
- Let $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ be cyclic groups with generators G_1, G_2, and $e(G_1, G_2)$ of prime order q, respectively, and $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be asymmetric pairing. $\mathbb{G}_v$ is specified by elliptic curve parameter $\mathcal{E}_v$ $(v = 1, 2)$ in [1], and pairing e is specified as in [2].
- Hash functions $H_v : \{0,1\}^* \to \mathbb{G}_v$ are defined as $H_v(M) = \text{HashingToPoint}(\mathcal{E}_v, \text{“FSU”}|| \text{ECP2OSP}(Z_1, R)||\text{ECP2OSP}(Z_2, R)||M)$ $(v = 1, 2)$. HashingToPoint is specified as in [3]. Key derivation function $H : \{0,1\}^* \to \{0,1\}^n$ is defined as $H(M) = \text{MGF1}(\text{“FSU”}|| \text{ECP2OSP}(Z_1, R)||\text{ECP2OSP}(Z_2, R)||M, n)$. MGF1 is specified as in [3]. Here, $Z_v \in \mathbb{G}_v$ $(v = 1, 2)$ are master public keys.

The master secret and public keys are generated as following.

- KGC randomly selects master secret key $z \in \mathbb{Z}_q$, and computes master public keys $Z_v = zG_v \in \mathbb{G}_v$ $(v = 1, 2)$.

The static secret keys are generated as following.

- For user U_i with identity ID_i, KGC generates static secret keys $D_{i,v} = zQ_{i,v} \in \mathbb{G}_v$ $(v = 1, 2)$, where $Q_{i,v} = H_v(ID_i)(= q_{i,v}G_v) \in \mathbb{G}_v$ $(v = 1, 2)$.

3 FSU protocol

U_A has identity ID_A and static secret key $D_{A,1} = zQ_{A,1} = zH_1(ID_A)(= zq_{A,1}G_1) \in G_1$. U_B has identity ID_B and static secret key $D_{B,2} = zQ_{B,2} = zH_2(ID_B)(= zq_{B,2}G_2) \in G_2$. Initiater U_A and responder U_B perform the following authenticated key exchange protocol. GroupMembershipTest is specified as in [3].

1. U_A selects a random ephemeral secret key $x_A \in_U \mathbb{Z}_q$, computes the ephemeral public key $X_{A,v} = x_A G_v$ $(v = 1, 2)$, computes $\hat{X}_{A,v} = \text{ECP2OSP}(X_{A,v}, R)$ $(v = 1, 2)$, and sends $(ID_A, ID_B, \hat{X}_{A,1}, \hat{X}_{A,2})$ to U_B.
2. Upon receiving $(ID_A, ID_B, \hat{X}_{A,1}, \hat{X}_{A,2})$, U_B computes $X_{A,v} = \text{OS2ECPP}(\hat{X}_{A,v})$ $(v = 1, 2)$, verifies $\text{GroupMembershipTest}(\mathcal{E}_v, X_{A,v}) = 1$ $(v = 1, 2)$ and $e(X_{A,1}, g_2) = e(g_1, X_{A,2})$, and aborts if not.

   U_B selects a random ephemeral secret key $x_B \in_U \mathbb{Z}_q$, computes the ephemeral public key $X_{B,v} = x_B G_v$ $(v = 1, 2)$, computes $\hat{X}_{B,v} = \text{ECP2OSP}(X_{B,v}, R)$ $(v = 1, 2)$, and sends $(ID_B, ID_A, \hat{X}_{B,1}, \hat{X}_{B,2})$ to U_A.

U_B computes shared values

$$\sigma_1 = e(Q_{A,1}, D_{B,2}), \sigma_2 = e(Q_{A,1} + X_{A,1}, D_{B,2} + x_B Z_2), \sigma_3 = x_B X_{A,1}, \sigma_4 = x_B X_{A,2},$$

computes $\hat{\sigma}_i = \mathrm{FE2OSP}(\sigma_i)$ $(i = 1, 2)$ and $\hat{\sigma}_i = \mathrm{ECP2OSP}(\sigma_i, R)$ $(i = 3, 4)$, computes the session key $K = H(\hat{\sigma}_1 || \hat{\sigma}_2 || \hat{\sigma}_3 || \hat{\sigma}_4 || sid)$, where $sid = (ID_A || ID_B || \hat{X}_{A,1} || \hat{X}_{A,2} || \hat{X}_{B,1} || \hat{X}_{B,2})$, and completes the session.

3. Upon receiving $(ID_B, ID_A, \hat{X}_{B,1}, \hat{X}_{B,2})$, U_A computes $X_{B,v} = \mathrm{OS2ECPP}(\hat{X}_{B,v})$ $(v = 1, 2)$, verifies $\textsc{GroupMembershipTest}(\mathcal{E}_v, X_{B,v}) = 1$ $(v = 1, 2)$ and $e(X_{B,1}, g_2) = e(g_1, X_{B,2})$, and aborts if not.

   U_A computes shared values

   $$\sigma_1 = e(D_{A,1}, Q_{B,2}), \sigma_2 = e(D_{A,1} + x_A Z_1, Q_{B,2} + X_{B,2}), \sigma_3 = x_A X_{B,1}, \sigma_4 = x_A X_{B,2},$$

   computes $\hat{\sigma}_i = \mathrm{FE2OSP}(\sigma_i)$ $(i = 1, 2)$ and $\hat{\sigma}_i = \mathrm{ECP2OSP}(\sigma_i, R)$ $(i = 3, 4)$, computes the session key $K = H(\hat{\sigma}_1 || \hat{\sigma}_2 || \hat{\sigma}_3 || \hat{\sigma}_4 || sid)$, where $sid = (ID_A || ID_B || \hat{X}_{A,1} || \hat{X}_{A,2} || \hat{X}_{B,1} || \hat{X}_{B,2})$, and completes the session.

Both parties compute the same shared values

$$\sigma_1 = e(G_1, G_2)^{z q_{A,1} q_{B,2}}, \sigma_2 = e(G_1, G_2)^{z(q_{A,1}+x_A)(q_{B,2}+x_B)}, \sigma_3 = x_A x_B G_1, \sigma_4 = x_A x_B G_2,$$

and compute the same session key K.

Appendix

A Sample Parameter

Sample parameter of FSU is as follows:

$$\begin{aligned} R &= \text{Compressed}, \\ Hash &= \text{SHA-256}, \\ n &= 32, \\ hashLen &= 32, \\ \mathcal{E}_1 &= \text{“Fp254BNp”}, \\ \mathcal{E}_2 &= \text{“Fp254n2BNp”}. \end{aligned}$$

The details of the Elliptic curve parameter Fp254BNp [1] is as follows:

- Carve-ID = Fp254BNp
- p_b = 0x2523648240000001ba344d80000000086121000000000013a700000000000013
- $p_e = u \in \mathbf{F}_{p_b}[u]$
- $A = 0$
- $B = 2$
- x = 0x2523648240000001ba344d80000000086121000000000013a700000000000012

- $y = 1$
- $q =$ 0x2523648240000001ba344d8000000007ff9f800000000010a10000000000000d
- $h = 1$

Elliptic curve parameter Fp254n2BNp [1] is as follows:

- Carve-ID = Fp254n2BNp
- $p_b =$ 0x2523648240000001ba344d80000000086121000000000013a700000000000013
- $p_e = u^2 + 1 \in \mathbf{F}_{p_b}[u]$
- $A = 0$
- $B = 1$
  $+$ (0x2523648240000001ba344d80000000086121000000000013a700000000000012)u
- $x =$ 0x061a10bb519eb62feb8d8c7e8c61edb6a4648bbb4898bf0d91ee4224c803fb2b
  $+$ (0x0516aaf9ba737833310aa78c5982aa5b1f4d746bae3784b70d8c34c1e7d54cf3)u
- $y =$ 0x021897a06baf93439a90e096698c822329bd0ae6bdbe09bd19f0e07891cd2b9a
  $+$ (0x0ebb2b0e7c8b15268f6d4456f5f38d37b09006ffd739c9578a2d1aec6b3ace9b)u
- $q =$ 0x2523648240000001ba344d8000000007ff9f800000000010a10000000000000d
- $h =$ 0x2523648240000001ba344d8000000008c2a2800000000016ad00000000000019

References

[1] K. Kasamatsu, S. Kanno, T. Kobayashi and Y. Kawahara: Barreto-Naehrig Curves draft-Kasamatsu-bncurves-01. Network Working Group Internet-Draft: (2014).

[2] K. Kasamatsu, S. Kanno, T. Kobayashi and Y. Kawahara: Optimal Ate Pairing draft-kasamatsu-optimal-ate-pairings-00. Network Working Group Internet-Draft: to apper.

[3] NTT Secure Platform Laboratories: Specification of Data Types and Conversions version 0. ¡https://info.isl.ntt.co.jp/crypt/index.html¿.

[4] Atsushi Fujioka, Fumitaka Hoshino, Tetsutaro Kobayashi, Koutarou Suzuki, Berkant Ustaoglu, Kazuki Yoneyama: id-eCK Secure ID-Based Authenticated Key Exchange on Symmetric and Asymmetric Pairing. IEICE Transactions 96-A(6): 1139-1155 (2013).

[5] ISO/IEC 11770-3:2014 Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques.