$\overline{}$	Style Definition: zzCopyright
\backslash	Style Definition: Footer
	Formatted: Different first page header
	Formatted: Font: Not Bold
$\overline{}$	Formatted: Font: Not Bold
\backslash	Formatted: Font: Not Bold
	Formatted: Font: Not Bold

2022-12-22

Final text for Date: 2023-02-0

JSO/IEC 20008-2:2013/Amd, 2:20222023(E)

ISO/IEC JTC1/SC 27/WG 2

Secretariat: DIN

Information technology — Security techniques —Anonymous digital signatures — Part 2: Mechanisms using a group public key — Amendment 2

Technologies de l'information — Techniques de sécurité — Signatures numériques anonymes –	-	Formatted: French (Switzerland)
<u>Partie 2 : Mécanismes utilisant une clé publique de groupe –</u>		Formatted: French (Switzerland)
Amendement		Formatted: French (Switzerland)

iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO/IEC 20008-2:2013/PRF Amd 2

https://standards.iteh.ai/catalog/standards/sist/cfd84dbf-ced8-4363-a0e0-269b5873e0b1/isoiec-20008-2-2013-prf-amd-2

Final text for ISO/IEC 20008-2:2013/Amd. 2:20222023(E)

© <u>ISO 20222023</u>		Formatted
All rights reserved. Unless otherwise specified, or required in the context of its implementation, no	\checkmark	Formatted: Default Paragraph Font
part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's ISO's member body in the country of the requester.		Formatted: Indent: Left: 0 pt, Right: 0 pt, Space Before: 0 pt, No page break before, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
ISO copyright officeCopyright Office		
CP 401 • Ch. de Blandonnet 8		
CH-1214 Vernier, Geneva		Formatted: Indent: Left: 0 pt, First line: 0 pt, Right: 0
Phone: +_41 22 749 01 11		pt, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Email: copyright@iso.org		
Email: copyright@iso.org		
Website: www.iso.org		Formatted: English (United Kingdom)
Published in Switzerland, 11en SIANDARD PK		Formatted: Indent: Left: 0 pt, First line: 0 pt, Right: 0 pt, Adjust space between Latin and Asian text, Adjust
	i) \\	space between Asian text and numbers Formatted: English (United Kingdom)
		Formatted: English (United Kingdom)

https://standards.iteh.ai/catalog/standards/sist/cfd84dbf-ced8-4363-a0e0-269b5873e0b1/iso iec-20008-2-2013-prf-amd-2

Formatted: Font: 11 pt

Formatted: Space After: 0 pt, Line spacing: single

2 © ISO/IEC 2022 – All rights reserved

ii

© ISO/IEC 2023 – All rights reserved

Edited DIS - MUST BE USED FOR FINAL DRAFT

Final text for ISO/IEC 20008-2:2013/Amd. 2:20222023(E)

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see <a href="http://www.iso.org/directiveswww.is

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iso.org/iso/foreword.html. In the IEC, see

https://standards.iten.ai/catalog/standards/sist/cid84dbf-ced8-4363-a0e0-269b5873e0b1/iso

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 20008 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at <u>www.iso.org/members.html</u>www.iso.org/members.html and <u>www.iec.ch/national-committees</u>.

Formatted: Font: 11 pt

Formatted: English (United Kingdom)

Formatted: Space After: 0 pt, Line spacing: single

© ISO/IEC 2022 – All rights reserved 3

© ISO/IEC 2023 – All rights reserved

Edited DIS - MUST BE USED FOR FINAL DRAFT

iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO/IEC 20008-2:2013/PRF Amd 2

https://standards.iteh.ai/catalog/standards/sist/cfd84dbf-ced8-4363-a0e0-269b5873e0b1/isoiec-20008-2-2013-prf-amd-2

<u>ISO/IEC 20008-2/Amd. 2:2023(</u>)	E] ≁	Formatted: Right
	T	
	+	-
		Formatted: Different first page header
Information technology — Security techniques — Anonymous		Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and
digital signatures — Part 2: Mechanisms using a group public		numbers
key — Amendment 2		
		Formatted: Font: Italic
Clause_4		
Add the following symbol:		
F(p) $F(p)$ the finite field containing exactly $p p$ elements.		Field Code Changed
		Field Code Changed
6.1		
Replace the first sentence with the following:		
This clause specifies five digital signature mechanisms with linking capability.		
Replace the text of NOTE 1 with the following:		
In the literature, the mechanism of 6.2 is called a list signature scheme, the mechanism of 6.6 is called	d	
a pre-DAA scheme and the mechanisms of 6.3, 6.4 and 6.5 are called DAA schemes. The mechanism	15	
given in 6.2, 6.4, 6.5 and 6.6 are based on schemes originally specified in References-[9], [6], [11] an [22] respectively, in which security proofs can also be found. The mechanism in 6.3 is based on		
scheme in Reference-[3] which is a minor modification of the scheme in Reference [4]; the associate		
security analysis is given in the full version of Reference-[4]. 08-2:2013/PRF Amd 2		
https://standards.iteh.ai/catalog/standards/sist/cfd84dbf-ced8-4363-	a0e0	
6.6 iec-20008-2-2013-prf-amd-2	I	
Add new subclause 6.6 as follows:		
nu new subclause 0.0 as follows.	1	
- 6.6 Mechanism 8	ļ	
6.6 Mechanism 8		
6.6.1 Symbols		
The following symbols apply in the specification of this mechanism.		Field Code Changed
$- \tau \tau$: a security parameter.	1	Field Code Changed
ΡΡ ΟΥΟΥ <u>νν'νς σρ'τ</u> ινν'νς σρ'τ		Field Code Changed
$-\frac{P_{1}P_{1}}{T_{2},K_{1},K_{2},K,K_{1}',K_{2}',K',J,T_{1}',T_{2}',R,R',T,T',R'',T''} \frac{Y_{1},X_{1}',\tilde{X}_{1},C_{1},D,D',T_{1}}{T_{2},K_{1},K_{2},K,K_{1}',K_{2}',K',J,T_{1}',T_{2}',R,R',T,T',R'',T''} T_{2},K_{1},K_{2},K,K_{1}',K_{2}',K',J,T_{1}',T_{2}',R,R',T,T',R'',T''} T_{2},K_{1},K_{2}',K,K_{1}',K_{2}',K',J,T_{1}',T_{2}',R,R',T,T',R'',T''} T_{2},K_{2},K,K_{1}',K_{2}',K',K',K',K',K',K',K',K',K',K',K',K',K'$	· /	Field Code Changed
$\frac{T_2,K_1,K_2,K,K_1,K_2,K',J,T_1,T_2,R,R',T,T',R'',T''}{T_2,K_1,K_2,K,K_1,K_2,K',J,T_1,T_2,R,R',T,T',R'',T''}$	":	Field Code Changed
elements of $G_{\Gamma}G_{1}$.		Field Code Changed
	$\top /$	Field Code Changed
$- \frac{P_2}{P_2}, \frac{X_2}{X_2}, \frac{X_2}{Y_2}, \frac{X_2}{X_2}, \frac{\tilde{X}_2}{X_2}, \frac{\tilde{X}_2}{X_2}, \frac{\tilde{X}_2}{X_2}: \text{ elements of } \frac{G_2}{G_2}.$		Field Code Changed
		Field Code Changed
		Field Code Changed
© ISO/IEC 2023 – All rights reserved	t	

2

_	x,y,z,x',z',c_k,s_x,s_z,c_k,s₁,u,v,w,v',r,s₂,k_r,k_x,k_z,c,z_r,z_x,z_z,c',s,l,k_s,c_m,p,c_m
	$x, y, z, x', z', c_k, s_x, s_z, c'_k, s_1, u, v, w, v', r, s_2, k_r, k_x, k_z, c, z_r, z_x, z_z, c', s, l, k_s, c_m, \rho, c'_m$: integers in $\frac{Z_p}{D}$
	<u>Z_p.</u>
—	$n_T n_I$: an integer of size $-\tau$ -bit.
_	$H_{\Gamma} H_{1}$: a hash function that outputs elements in $G_{\Gamma} G_{1}$.
_	$H_{\overline{Z}}H_{2}$, $H_{\overline{3}}H_{3}$: hash functions that output elements in $\frac{Z_{\overline{p}}}{Z_{p}}$.
_	
6.6	2– <u>Key generation process</u>
setu pub pro	e key generation process has two parts: setup process and group membership issuing process. The up process is executed by the group membership issuer to create the group public parameter, group olic key, and group membership issuing key. The group membership issuing process is an interactive tocol running between the group membership issuer and a group member to create a unique group mber signature key for the group member.
The	setup process takes the following steps by the group membership issuer:
a)	Choose $\pm \underline{\tau}$ as a security parameter.
b)	Choose a bilinear group pair $(\frac{G_1}{G_1}, \frac{G_2}{G_2}, \frac{G_2}{G_2})$ of large prime order $p \cdot p$, such that no efficiently
	computable homomorphism is known between $G_1 G_1$ and $G_2 G_2$, in either direction, and an
	associated pairing function $e: \mathcal{C}_{T} \mathcal{C}_{1} \times \mathcal{C}_{Z} \mathcal{C}_{2} \to \mathcal{C}_{T} \mathcal{C}_{T}$. The constraint of the const
c)	Choose two random independent generators $P_{T}P_{1}$ and $Q_{T}Q_{1}$ of $G_{T}G_{1}$ and provide additional
	information, denoted by $\pi_{\text{Gen}} \pi_{\text{Gen}}$, that serve to demonstrate that these two generators were
	indeed chosen independently, that is without a potentially exploitable relationship between them (such as $Q_{\Gamma}Q_{1} = \frac{[s]P_{\Gamma}[s]P_{1}}{[s]P_{1}}$ for an integer <u>s-s</u> chosen by the group membership issuer). An
	example of how to verifiably select independent generators and to verify, using $\pi_{\text{Gen}} \pi_{\text{Gen}}$, the
	correct generation of these generators, is given in Annex G.
d)	Choose a random generator $P_{Z} P_{2}$ of $G_{Z} G_{2}$.
e)	Choose three hash functions $H_{\overline{1}}H_{1}: \overline{\{0,1\}}^{*} \overline{\{0,1\}}^{*} \rightarrow G_{\overline{1}}G_{1}, H_{\overline{2}}H_{2}: \overline{\{0,1\}}^{*} \overline{\{0,1\}}^{*} \rightarrow \overline{Z_{p}}Z_{p}$ and H_{3}
	$H_3: \{0,1\}^* \{0,1\}^* \to \mathbb{Z}_p Z_p$. An example of how to construct such hash functions is provided in
	Annex B.
f)	Choose three random integers $\frac{x}{x}, \frac{y}{y}$ and $\frac{z}{z}$ in $\frac{z}{p}Z_p$.
2	© ISO/IEC 2022 – All rights reserved

Field Code Changed **Field Code Changed** Field Code Changed **Field Code Changed** Field Code Changed **Field Code Changed** Field Code Changed Formatted: Font: 11 pt

Formatted: Space After: 0 pt, Line spacing: single

Orange Restricted

© ISO/IEC 2023 - All rights reserved

<u>ISO/IEC 20008-2/Amd. 2:2023(E</u>	•	Formatted: Right	
g) Compute $X_{\Gamma} = [z]P_{\Gamma} + [x]Q_{\Gamma}, Y_{\Gamma} = [y]P_{\Gamma}, X_{2} = [x]P_{2} \text{ and } Y_{2} = [y]P_{2}.$			
g) Compute $X_1 = [z]P_1 + [x]Q_1 + Y_1 = [y]P_1 + X_2 = [x]P_2$ and $Y_2 = [y]P_2$.		Field Code Changed	
h) Choose two random integers $\frac{x'x'}{x}$ and $\frac{z'z'}{z}$ in $\frac{Z_p}{Z_p}$.		Field Code Changed	
i) Compute $X'_1 = [z']P_1 + [x']Q_1$ and $X'_2 = [x']P_2$.			
$\frac{1}{2} \text{Compute } c_k = -H_2(P_1 Q_1 P_2 X_1 Y_1 X_2 Y_2 X_1 X_2 Y_2 X_1 X_2 Y_2 X_1 X_2 Y_2 Y_$			
k) Compute $s_x = \{x' - + -c_k - x \cdot x\} \mod p$ and $s_z = \{z' - + -c_k - x \cdot z\} \mod p$.			
<u>i) Compute $X'_1 = [z']P_1 + [x']Q_1$ and $X'_2 = [x']P_2$.</u>		Field Code Changed	
<u>i) Compute $c_{k} = H_2(P_1 _P_2 _P_2 _Y_1 _Y_1 _Y_2 _Y_2$</u>		Field Code Changed	
k) Compute $s_x = (x'_+, c_k \times x) \mod p$ and $s_z = (z'_+, c_k \times z) \mod p$.		Field Code Changed	
l) Set $\pi_{\text{val}} = (c_k, s_x, s_z) \pi_{\text{val}} = (c_k, s_x, s_z)$ as a proof that the second component of the representation of $X_T X_1$ in the base $P_T P_1$ and $Q_T Q_1$ is equal to the discrete logarithm of $X_Z X_2$ in the base $P_Z P_2$.		Field Code Changed	
m) Output the following:			
- group public parameter = $(G_{1}, G_{2}, G_{2}, G_{T}, e_{e}, P_{1}, P_{1}, Q_{1}, P_{2}, P_{2}, P_{p}, H_{1}, H_{1}, H_{2}, H_{2}, H_{3}, H_{3}),$		Field Code Changed 269b5873e0b1/iso-	
$- \text{ group public key} = (\frac{X_T}{X_1}, \frac{Y_T}{Y_1}, \frac{X_Z}{X_2}, \frac{Y_Z}{Y_2}, \frac{\pi_{\text{Gen}}}{\pi_{\text{Val}}}, \frac{\pi_{\text{Val}}}{Y_2}, \frac{\pi_{\text{Gen}}}{\pi_{\text{Val}}}, \frac{\pi_{\text{Val}}}{Y_2}).$		Field Code Changed	
— group membership issuing key = $(\frac{x, y, z, x, y, z}{x, y, z})$.		Field Code Changed	
NOTE 1 Examples of recommended parameters are provided in C.2.			
Each entity involved in this anonymous signature mechanism should verify the validity of the group public key before using it. The group public key validity verification process includes the following steps			
a) Verify that $P_{T} P_{1}$ and $Q_{T} Q_{1}$ were generated independently using π_{Gen} .		Field Code Changed	
b) Verify the validity of the proof π_{val} :		Field Code Changed Field Code Changed	
1) Compute $\tilde{X}_1 = [s_z]P_1 + [s_x]Q_1 - [c_k]X_1$ and $\tilde{X}_2 = [s_x]P_2 - [c_k]X_2$.			
<u>1) Compute $\tilde{X}_1 = [s_z]P_1 + [s_x]Q_1 = [c_k]X_1$ and $\tilde{X}_2 = [s_x]P_2 = [c_k]X_2$.</u>		Field Code Changed Formatted: Font: 11 pt	
© ISO/IEC 2022 – All rights reserved 3		Formatted: Space After: 0 pt, Line spacing: sir	ngle
© ISO/IEC 2023 – All rights reserved Orange Restricted			
	_		

	2) Compute $\dot{c_k} = H_2 \left(P_1 \parallel Q_1 \parallel P_2 \parallel X_1 \parallel Y_1 \parallel X_2 \parallel Y_2 \parallel \tilde{X}_1 \parallel \tilde{X}_2 \right).$			
	3) Verify that $\frac{c_k}{c_k} = \frac{c_k}{c_k}$.		Field Code Changed	
c)	Verify that $e \underbrace{e(\underline{Y}_1, \underline{Y}_1, \underline{P}_2, \underline{P}_2)}_{=} = e(\underbrace{P_1}_{\underline{P}_1}, \underbrace{Y_2}_{\underline{Y}_2}Y_2).$		Field Code Changed	
	If any of the above verifications fails, output 0 (invalid), otherwise output 1 (valid).			
me	e group membership issuing process requires a secure and authentic channel between the group ember and the group membership issuer. How to establish such a channel is out scope of this echanism. The group membership issuing process includes the following steps:			
a)	The group membership issuer chooses a nonce $n_{I_{\underline{n}}} \in \underbrace{\{0,1\}^{T}}_{\underline{n}} \{0,1\}^{T}$.		Field Code Changed	
b)	The group membership issuer sends $\frac{n_I}{n_I}$ to the member.		Field Code Changed	
c)	The member chooses a random integer $\frac{s_T s_1}{z_p Z_p}$.		Field Code Changed	
d)	The member computes $C_{T} C_{1} = [s_{1}]Y_{T}[s_{1}]Y_{1}$.		Field Code Changed	
e)			Field Code Changed	
f)	The member computes $\mathcal{P}\underline{D} = \underline{[u]Y_1}[u]Y_1$. <u>ISO/IEC 20008-2:2013/PRF Amd 2</u>		Field Code Changed	
g)	$- \frac{1}{2} + $			
	The member computes $v_{\underline{-}} = H_2(P_1 \parallel Q_1 \parallel P_2 \parallel X_1 \parallel Y_1 \parallel X_2 \parallel Y_2 \parallel C_1 \parallel \underline{D} \parallel \underline{n_l}).$		Field Code Changed	
	The member computes $w w = = (w u + + v \times s_1 \times s_1) \mod p$.		Field Code Changed	
i)	The member sends $(\mathcal{L}_{T}\mathcal{L}_{1}, \psi v, \psi w)$ to the group membership issuer.		Field Code Changed	
j)	The group membership issuer computes $\frac{D'}{D'} = \frac{[w]Y_1[w]Y_1}{[w]Y_1} - \frac{[v]C_1[v]C_1}{[v]C_1}$.		Field Code Changed	
k)	The group membership issuer computes $v' v' = H_Z H_2 (P_T P_1 Q_T Q_1 P_Z P_2 X_T X_1 Y_T Y_1 X_Z$	Λ	Field Code Changed	
	$\underline{X_2} \underline{Y_2} \underline{Y_2} \underline{C_1} \underline{C_1} \underline{\mathcal{D}}' \underline{\underline{D}'} \underline{n_1} \underline{n_1}).$			
l)	The group membership issuer verifies $\psi v = v'v'$. If the verification fails, abort the group membership issuing process.	_	Field Code Changed	
		1	Formatted: Font: 11 pt Formatted: Space After: 0 pt, Line spacing:	single
4	© ISO/IEC 2022 – All rights reserved			single
4	© ISO/IEC 2023 – All rights reserved			
	Orange Restricted	/		

	<u>ISO/IEC 20008-2/Amd. 2:2023(E</u>)←		Formatted: Right	
m)	The group membership issuer selects five random integers $\frac{r}{r}, \frac{s_z}{s_z}, \frac{k_r}{k_r}, \frac{k_x}{k_x}$ and $\frac{k_z}{k_z}$ from $\frac{z_p}{z_p}$.	/	Field Code Changed	
n)	The group membership issuer computes $T_{T_1} = [r]P_{T_1}[r]P_1$ and $T_{Z_2} = [x]T_{T_1}[x]T_1 + [r]C_1 + [r]C_1 + [r \times s_2]Y_{T_1}[r \times s_2]Y_1$.	1	Field Code Changed)
0)	The group membership issuer computes $\frac{K_T K_1}{K_1} = \frac{[k_r]P_T[k_r]P_1}{[k_r]P_1}, \frac{K_Z K_2}{K_Z} = \frac{[k_x]T_T[k_x]T_1}{[k_x]T_1} + \frac{[k_r](C_1 + [s_2]Y_1)[s_2]Y_1}{[s_2]Y_1}$ and $\frac{K_K}{K} = \frac{[k_x]P_T[k_x]P_1}{[k_x]P_1} + \frac{[k_x]Q_T[k_x]Q_1}{[k_x]Q_1}.$	1	Field Code Changed	
p)	The group membership issuer computes $c = H_2 c = H_2 (P_T P_1 Q_T Q_1 P_Z P_2 X_T X_1 Y_T Y_1 X_T X_2 Y_Z Y_2 C_T C_1 S_Z S_2 K_T K_1 K_Z K_2 K K).$	1	Field Code Changed	
q)	The group membership issuer computes $z_r = \{k_r \cdot + \cdot c_x \cdot r\} \mod p_r \cdot z_x = \{k_x \cdot + \cdot c_x \cdot x\} \mod p_r$ and $z_z = \{k_z \cdot + \cdot c_x \cdot z\} \mod p_r$.			
<u>q)</u>	The group membership issuer computes $z_{r} = (k_r + c \times r) \mod p_{r} z_{x} = (k_x + c \times x) \mod p_{r}$ and $z_{z} = (k_z + c \times z) \mod p_{x}$	1	Field Code Changed)
r)	The group membership issuer sets (T_T, T_1, T_2, T_2) as the member's group membership credential and sends $(T_T, T_1, T_2, s_2, c, z_r, z_x, z_z, T_2, s_2, c, z_r, z_x, z_z)$ to the member.	1	Field Code Changed	
	iec-20008-2-2013-prf-amd-2			
	$- \text{The member computes-} \tau' - = -H_2 (P_1 -Q_1 -P_2 -X_1 -Y_1 -X_2 -Y_2 -C_1 -S_2 -K_1 -K_2 -K_2 $			
<u>s)</u>	The member computes $K'_1 = [z_r]P_1 - [c]T_1 - K'_2 = [z_x]T_1 + [z_r](C_1 + [s_2]Y_1) - [c]T_2$ and $K' = \underbrace{[z_z]P_1 + [z_x]Q_1 = [c]X_1}_{z_1}$	1	Field Code Changed)
<u>t)</u>	<u>The member computes $\underline{c'} = H_2(P_1 \parallel Q_1 \parallel P_2 \parallel X_1 \parallel Y_1 \parallel X_2 \parallel Y_2 \parallel C_1 \parallel s_2 \parallel K_1 \parallel K_2 \parallel K_1).$</u>		Field Code Changed	
	The member verifies $\frac{c}{c} = \frac{c'}{c'} \frac{c'}{c'}$. If the verification fails, the member aborts.	_	Field Code Changed	
v)	The member computes $\frac{s}{s} = \frac{s_1}{s_1} + \frac{s_2}{s_2} = \frac{s_1}{s_1} + \frac{s_1}{s_2} = \frac{s_1}{s_1} + \frac{s_2}{s_2} = \frac{s_1}{s_1} + \frac{s_2}{s_2} = \frac{s_1}{s_1} + \frac{s_2}{s_2} = \frac{s_1}{s_1} + \frac{s_2}{s_2} = \frac{s_1}{s_1} + \frac{s_1}{s_2} = \frac{s_1}{s_1} + \frac{s_2}{s_2} = \frac{s_1}{s_1} + \frac{s_1}{s_2} = \frac{s_1}{s_1} + \frac{s_2}{s_2} = \frac{s_1}{s_1} + \frac{s_2}{s_2} = \frac{s_1}{s_1} + \frac{s_1}{s_2} $		Field Code Changed	
w)	The group member signature key for the member is $(\underbrace{s}_{2}, \underbrace{T_{1}}_{T_{1}}, \underbrace{T_{2}}_{T_{2}})$.		Field Code Changed	
	TTE 2 The group membership issuer can use the same value $s_2 s_2$ (for example $s_2 = 0 \text{ mod } p p$) for veral executions of the group membership issuing process. In this case, the security of Mechanism 8 relies on the		Field Code Changed (Formatted: Font: 11 pt (Formatted: Space After: 0 pt, Line spacing: single (
© IS	SO/IEC 2022 – All rights reserved 5			
<u>© IS</u>	SO/IEC 2023 – All rights reserved 5			

Pointcheval-Sanders (PS) assumption^[24], instead of the q-MSDH assumption^[25] if the group membership issuer uses a fresh random value $\frac{s_2}{s_2} s_2$ for each new session of the group membership issuing process.

6.6.3 Signature process

I

On input of a group member signature key $(\underline{s}, \underline{s}, \underline{T_1}, \underline{T_2}, \underline{T_2})$, a linking base <u>bsn</u> and a message <u>m</u>	1	Field Code Changed
$\underline{m} \in \underline{(0,1)}^* \{0,1\}^*$ to be signed, the signature process takes the following steps. The linking base,		
denoted by $\frac{bsn}{bsn}$, is either a special symbol \perp or an arbitrary string used for the linking capability.		
a) If $bsn = \underline{I}$, the signer chooses a random \underline{J} from $\underline{G_{T}}G_{1}$, otherwise, computes $\underline{J} = \underline{H_{T}}H_{1}$	1	Field Code Changed
bsn bsn).		
b) The signer selects two random integers $+\underline{l}$ and $\underline{k_s} k_s$ in $\underline{Z_p} \underline{Z_p}$.	1	Field Code Changed
c) The signer computes $\overline{T_1} \underline{T_1} = \underline{[l]} \overline{T_1} \underline{[l]} T_1$ and $\overline{T_2} \underline{T_2} = \underline{[l]} \overline{T_2} \underline{[l]} T_2$.	1	Field Code Changed
d) The signer computes $\frac{R}{R} = \frac{s}{r_1} \frac{r_1}{s} \frac{s}{r_1} \frac{r_1}{s} \frac{s}{r_1} \frac{r_2}{s} \frac{s}{r_1} \frac{r_2}{s} \frac{s}{r_1} \frac{r_2}{s} \frac{s}{r_1} \frac{r_2}{s} \frac{s}{r_1} \frac{s}{s} \frac{r_2}{r_1} \frac$	1	Field Code Changed
e) The signer computes $\mathcal{T} = [s]J = [s]J$ and $\mathcal{T}' = [k_s]J = [k_s]J$.	1	Field Code Changed
f) The signer computes $\epsilon_m c_m = \frac{H_3}{4} H_3 (\overline{T_1} T_1 \overline{T_2} T_2 J T T_1 \overline{R_R} \overline{R_R} T T_1 \overline{R_R} R_$	1	Field Code Changed
g) The signer computes $p = (k_s k_s + c_m \times s c_m \times s) \mod p p$.		Field Code Changed
h) The signer outputs the anonymous signature $\sigma = (T_1, T_1, T_2, T_2, J, R, T, c_m, \rho)$.	1	Field Code Changed
- 6.6.4 Verification process		
On input of a message $\frac{m}{m}$, a linking base $\frac{bsn}{bsn}$, a signature $(\frac{T_1}{T_1}T_1, \frac{T_2}{T_2}T_2, \frac{J,R,T,c_m,\rho}{T_1})$	1	Field Code Changed
J,R,T,c_m,ρ and a group public key $(X_{\Gamma}X_1, Y_{\Gamma}Y_1, X_ZX_2, Y_ZY_2)$, the verification process takes the	/	
following steps:		
a) If $bsn \neq \pm$, verify that $J = -H_1(bsn)$.		
a) If $bsn_{\neq} \perp$ verify that $J_{=} H_1(bsn)$.	1	Field Code Changed
b) Verify that $\frac{T_1 \neq O_E}{T_1 \neq O_E}$.	1	Field Code Changed
c) If any of the above verifications fails, output 0 (invalid).	ĥ	Formatted: Font: 11 pt
€© ISO/IEC 2022 – All rights reserved		Formatted: Space After: 0 pt, Line spacing: single
6 © ISO/IEC 2023 – All rights reserved Orange Restricted		
	7	

field Code Changed g) Verify that $\frac{1}{2m}(\underline{r}_1, \underline{r}_2) = e(T_2, \underline{r}_2)$. h) Verify that $\frac{1}{2m}(\underline{r}_1, \underline{x}_2) = e(T_2, \underline{r}_2)$. h) Verify that $e(T_1, \underline{x}_2) = e(T_2, \underline{r}_2)$. h) Verify that $e(T_1, \underline{x}_2) = e(T_2, \underline{r}_2)$. h) Verify that $e(T_1, \underline{x}_2) = e(T_2, \underline{r}_2)$. h) Verify that $e(T_1, \underline{x}_2) = e(T_2, \underline{r}_2)$. h) Verify that $e(T_1, \underline{x}_2) = e(T_2, \underline{r}_2)$. h) Verify that $e(T_1, \underline{x}_2) = e(T_2, \underline{r}_2)$. i) Optionally, call the revocation checking process. i) If any of the above verifications (steps g and h) fails, output 0 (invalid), otherwise). Otherwise, output 1 (inkid). 6.5 Linking process Given two valid signatures $e_{\underline{\sigma}} = = (\underline{\tau}_1, \underline{\tau}_1, \underline{\tau}_2, \underline{\tau}_2, \underline{t}, \underline{h}, \overline{T}, \underline{e_m}, p)$ and $\underline{\phi} = (\underline{\phi}_1, \underline{\tau}_1, \underline{\tau}_1, \underline{\tau}_2)$ a) $it_1 - \underline{f} = \underline{f}$ and $T - \underline{e}, \underline{\hat{T}}$ output 1 (linked), otherwise, output 0 (not linked). NOTE If the linking process outputs 0 because of $\underline{f} \pm \underline{\hat{\tau}}, \underline{f} \pm \underline{\hat{f}}, \underline{\hat{\tau}}$, the mans that the linking process cannot determine whether two signatures were created by the same group member. 6.6 Revocation process b Details of the revocation process in this mechanism are surveyed in Reference [10]. There are two types of revocation can be either global revocation or local revocation. Verifier blacklist revocation is a local revocation.		ISO/IEC 20008-2/Amd. 2:2023(E	•	Formatted: Right	
e) Compute $\forall + \underline{r}_{-} = \{p_1\}_{-} = \{p_2\}_{-} = \{p_2\}_{-} = \{p_1\}_{-} = \{p_2\}_{-} = \{p_2\}_{-} = \{p_2\}_{-} = \{p_1\}_{-} = \{p_2\}_{-} = \{p$	d) Compute $\frac{R^*}{R}R'' = \frac{1}{12} \frac{1}{2} \frac{1}{2} \left[\rho \right] T_1' - \frac{1}{12} \frac{1}{2} \frac$			Field Code Changed	
6) Compute $\vec{\tau}_m = H_2(\vec{\tau}_1 \parallel \vec{\tau}_2 \parallel f \parallel \vec{\tau}_1 \parallel $					
Compute $c_{m,m} = H_2(T_1 \parallel T_2 \parallel f \parallel \Pi T_1 \parallel f \parallel H T_1 H H H H H H H H H H H H H H H H H H H$	e) Compute $\underline{T''} = [\rho]J = [\rho]J - [c_m]T [c_m]T$.			Field Code Changed	
g) Verify that $e_{in} e_{in} = e_{in} = e_{in}$. Field Code Changed Field Code Cha	f) Compute $c'_m = H_3(T'_1 T'_2 J T R T'' R'' m).$				
h) Verify that $e(T_1, X_2) = e(T_1, Y_2) = e(T_2, P_2)$ h) Verify that $e(T_1, X_2) = e(T_1, Y_2) = e(T_2, P_2)$ i) Optionally, call the revocation checking process. i) Orany of the above verifications (steps g and h) fails, output 0 (invalid), otherwise). Otherwise, output 1 (valid). 6.5 6.5 Linking process Given two valid signatures $e_{cr} = = (T_1^+T_1, T_2^-T_2, +B, T, c_m, \rho)$ and $\hat{\sigma}_{cr} = = (T_1^+T_1, T_2^-T_2, +B, T, c_m, \rho)$ and $\hat{\sigma}_{cr} = = (T_1^+T_1, T_2^-T_2, -B, T, c_m, \rho)$ and $\hat{\sigma}_{cr} = = (T_1^+T_1, T_2^-T_2, -B, T, c_m, \rho)$ and $\hat{\sigma}_{cr} = = (T_1^+T_1, T_2^-T_2, -B, T, c_m, \rho)$ and $\hat{\sigma}_{cr} = = (T_1^+T_1, T_2^-T_2, -B, T, c_m, \rho)$ and $\hat{\sigma}_{cr} = = (T_1^+T_1, T_2^-T_2, -B, T, c_m, \rho)$ and $\hat{\sigma}_{cr} = = (T_1^+T_1, T_2^-T_2, -B, T, c_m, \rho)$ and $\hat{\sigma}_{cr} = = (T_1^+T_1, T_2^-T_2, -B, T, c_m, \rho)$ and $\hat{\sigma}_{cr} = = (T_1^+T_1, T_2^-T_2, -B, T, c_m, \rho)$ and $\hat{\sigma}_{cr} = = (T_1^+T_1, T_2^-T_2, -B, T, c_m, \rho)$ and $\hat{\sigma}_{cr} = = (T_1^+T_1, T_2^-T_2, -B, T, c_m, \rho)$ and $\hat{\sigma}_{cr} = = (T_1^+T_1, T_2^-T_2, -B, T, c_m, \rho)$ and $\hat{\sigma}_{cr} = = (T_1^+T_1, T_2^-T_2, -B, T, c_m, \rho)$ and $\hat{\sigma}_{cr} = = (T_1^+T_1, T_2^-T_2, -B, T, c_m, \rho)$ and $\hat{\sigma}_{cr} = = (T_1^+T_1, T_2^-T_2, -B, T, T_1, T_2^-T_2, -B, T, $	<u>f) Compute $c_{m} = H_3(T_1 T_2 J T R T' R' R' m).$</u>			Field Code Changed	
h) Verify that $e(T_1, X_2) \times e(R, Y_2) = e(T_2, P_2)$. i) Optionally, call the revocation checking process. i) If any of the above verifications (steps g and h) fails, output 0 (invalid), otherwise). Otherwise, output 1 (valid). 6.5.5 Linking process Given two valid signatures $\sigma_{\underline{c}} = (c\overline{T}_1 T_1, \overline{T}_2 T_2, f.R, \overline{T}, c_{\underline{m}}, p)$ and $\hat{\sigma} \hat{\sigma} = (c\overline{T}_1 T_1, T_2 T_2), f.R, \overline{T}, c_{\underline{m}}, p)$ and $\hat{\sigma} \hat{\sigma} = (c\overline{T}_1 T_1, T_2 T_2), f.R, \overline{T}, c_{\underline{m}}, p)$ and $\hat{\sigma} \hat{\sigma} = (c\overline{T}_1 T_1, T_2 T_2), f.R, \overline{T}, c_{\underline{m}}, p)$ and $\hat{\sigma} \hat{\sigma} = (c\overline{T}_1 T_1, T_2 T_2), f.R, \overline{T}, c_{\underline{m}}, p)$ and $\hat{\sigma} \hat{\sigma} = (c\overline{T}_1 T_1, T_2 T_2), f.R, T, c_{\underline{m}}, p)$ and $\hat{\sigma} \hat{\sigma} = (c\overline{T}_1 T_1, T_2 T_2), f.R, T, c_{\underline{m}}, p)$ and $\hat{\sigma} \hat{\sigma} = (c\overline{T}_1 T_1, T_2 T_2)$ output 1 (linked), otherwise, output 0 (not linked)) if $f = \frac{1}{2}$ and $T + \frac{1}{2} + \frac{1}{2}$ output 1 (linked), otherwise, output 0 (not linked)) NOTE If the linking process to because of $f + \frac{1}{2} + \frac{1}{2}$, it means that the linking process cannet determine whether two signatures were created by the same group member. - - - - - - - - - - - - -	g) Verify that $\frac{c_m}{c_m} = c_m = c_m$.			Field Code Changed	
i) Optionally, call the revocation checking process. i) If any of the above verifications (steps g and h) fails, output 0 (invalid), otherwise). Otherwise, output 1 (valid). 6.6.5 Linking process Given two valid signatures $\sigma_{\underline{\sigma}} = \equiv (\hat{\tau}_1 \hat{\tau}_1, \hat{\tau}_2 \hat{\tau}_2, \hat{f}, \hat{h}, \hat{\tau}, \hat{c}_m, \hat{p})$ and $\hat{\tau}_{\underline{D}} = \equiv (\hat{\tau}_1 \hat{\tau}_1, \hat{\tau}_1, \hat{\tau}_2, \hat{\tau}, \hat{h}, \hat{h}, \hat{\tau}, \hat{c}_m, \hat{p})$, $\hat{h}, \hat{h}, \hat{c}_m, \hat{p}$), $\hat{h}, \hat{h}, \hat{c}_m, \hat{p}$) the linking process takes the following steps: a) $If J = \hat{J} = \hat{J}$ and $T = \hat{T} \hat{T}$, output 1 (linked), otherwise, output 0 (not linked). NOTE If the linking process outputs 0 because of $J \neq \hat{\tau} \hat{f} \neq \hat{J}$, it means that the linking process cannot determine whether two signatures were created by the same group member. 6.6.6 Revocation process Details of the revocation nal verifier blacklist revocation. Verifier blacklist revocation is a local revocation. Private key revocation and verifier blacklist revocation. Verifier blacklist revocation is a local revocation. Private key revocation list RL of this type. If a group member signature key ($\epsilon_S, \frac{x}{T}, \underline{T}_1, \frac{x}{T}, \underline{T}_2$) is compromised, the group membership issuer puts ϵ_S into a revocation list RL of this type. Field Code Changed Field Code Changed Field Code Changed	h) Verify that $e(T'_1, X_2) \times e(R, Y_2) = e(T'_2, P_2)$.				
i) If any of the above verifications (steps g and h) fails, output 0 (invalid), etherwise). Otherwise, output 1 (valid). 6.6.5 Linking process Given two valid signatures $\sigma_{\underline{\sigma}} = (\hat{\tau}_1 \hat{\tau}_1, \hat{\tau}_2 \hat{\tau}_2, \hat{f}_1 \hat{R}, \hat{T}, c_m, \rho)$ and $\hat{\tau}_{\underline{\sigma}} = (\hat{\tau}_1 \hat{\tau}_1, \hat{\tau}_1, \hat{\tau}_2, \hat{\tau}_2, \hat{f}_1 \hat{R}, \hat{\tau}, c_m, \rho)$ and $\hat{\tau}_{\underline{\sigma}} = (\hat{\tau}_1 \hat{\tau}_1, \hat{\tau}_1, \hat{\tau}_2, \hat{\tau}_2, \hat{f}_1 \hat{R}, \hat{\tau}, c_m, \rho)$ and $\hat{\tau}_{\underline{\sigma}} = (\hat{\tau}_1 \hat{\tau}_1, \hat{\tau}_1, \hat{\tau}_2, \hat{\tau}_2, \hat{f}_1 \hat{R}, \hat{\tau}, c_m, \rho)$ and $\hat{\tau}_{\underline{\sigma}} = (\hat{\tau}_1 \hat{\tau}_1, \hat{\tau}_1, \hat{\tau}_2, \hat{\tau}_2, \hat{f}_1 \hat{R}, \hat{\tau}, c_m, \rho)$ and $\hat{\tau}_{\underline{\sigma}} = (\hat{\tau}_1 \hat{\tau}_1, \hat{\tau}_1, \hat{\tau}_2, $	<u>h) Verify that $e(T_1, X_2) \times e(R, Y_2) = e(T_2, P_2)$.</u>			Field Code Changed	
1 (valid). 6.5. Linking process Given two valid signatures $e_{\underline{\sigma}} = = (\underline{\tau}_{1} \underline{\tau}_{1}, \underline{\tau}_{2} \underline{\tau}_{2}, \underline{f}, \underline{h}, \overline{t}, \underline{c}_{m}, p)$ and $\underline{+}_{2} \underline{+}_{2} = (\underline{\tau}_{1} \underline{\tau}_{1}, \underline{f}, \underline{\tau}_{2})$ $\vec{f}_{2}, \underline{f}, \underline{h}, \underline{f}, \underline{+}_{m}, p, \underline{f}, \underline{h}, \underline{\tau}, \underline{c}_{m}, p)$ the linking process takes the following steps: a) $ I_{f} = \underline{f} = \underline{f}$ and $T = \underline{\pm} \underline{+} \underline{\hat{T}}$ output 1 (linked), otherwise, output 0 (not linked). NOTE If the linking process outputs 0 because of $J = \underline{\pm} \underline{f} \underline{f} = \underline{\hat{f}}$, it means that the linking process cannot determine whether two signatures were created by the same group member. - 6.6.6 Revocation process Details of the revocation and verifier blacklist revocation) supported in this mechanism. Private key revocation. Private key revocation If a group member signature key ($\underline{+} \underline{s}, \underline{\tau}_{1} \underline{\tau}_{1}, \underline{\tau}_{2} \underline{\tau}_{2}$) is compromised, the group membership issue puts $\underline{+} \underline{s}$ into a revocation list RL of this type. Field Code Changed Field Code Changed	i) Optionally, call the revocation checking process.		l		
Given two valid signatures $\neq \underline{\sigma} = \underline{=} (\hat{\tau}_{1} T_{1}, \hat{\tau}_{2} T_{2}, f, R, T, c_{m}, \rho)$ and $\hat{\tau}, \hat{\sigma} = \underline{=} (\hat{\tau}_{1}, \hat{T}_{1}, \hat{\tau}_{2})$ $\hat{T}_{2}, \hat{f}, \hat{R}, \hat{\tau}, \hat{c}_{m}, \hat{\rho}), \hat{R}, \hat{T}, \hat{c}_{m}, \hat{\rho})$, the linking process takes the following steps: a) If $J = \hat{f} = \hat{f}$ and $T = \underline{=} \hat{T}, \hat{T}_{2}$ output 1 (linked), otherwise, output 0 (not linked). NOTE If the linking process outputs 0 because of $J \neq \hat{\tau}, \hat{f} \neq \hat{f}$, it means that the linking process cannot determine whether two signatures were created by the same group member. - 6.6 Revocation process Details of the revocation and verifier blacklist revocation) supported in this mechanism. Private key revocation can be either global revocation or local revocation. Verifier blacklist revocation is a local revocation: - If a group member signature key ($\pm s, \frac{x_{T}}{T_{1}}, \frac{x_{T}}{T_{2}}$) is compromised, the group membership issue puts $\pm s$ into a revocation list RL of this type. Field Code Changed Field Code Ch		(invalid), otherwise]. Otherwise , outpu	tR		
 a) If J = J = J and T = = T J, output 1 (linked), otherwise, output 0 (not linked). NOTE If the linking process outputs 0 because of J ≠ ∓ J = J , it means that the linking process cannot determine whether two signatures were created by the same group member. 6.6.6 Revocation process Details of the revocation process in this mechanism are surveyed in Reference [10]. There are two types of revocation process in this mechanism are surveyed in Reference [10]. There are two types of revocation can be either global revocation. Verifier blacklist revocation is a local revocation. Private key revocation: If a group member signature key (+ s, T₁ T₁, T₂ T₂) is compromised, the group membership issue puts + s into a revocation list RL of this type. Field Code Changed Formatted: Font: 11 pt Formatted: Space After: 0 pt, Line spacing: single OSO/IEC 2022 - All rights reserved 7 OSO/IEC 2023 - All rights reserved 	6.6.5 Linking process (Stand		l		
 a) If J = J = J and T = = T J, output 1 (linked), otherwise, output 0 (not linked). NOTE If the linking process outputs 0 because of J ≠ ∓ J = J , it means that the linking process cannot determine whether two signatures were created by the same group member. 6.6.6 Revocation process Details of the revocation process in this mechanism are surveyed in Reference [10]. There are two types of revocation process in this mechanism are surveyed in Reference [10]. There are two types of revocation can be either global revocation. Verifier blacklist revocation is a local revocation. Private key revocation: If a group member signature key (+ s, T₁ T₁, T₂ T₂) is compromised, the group membership issue puts + s into a revocation list RL of this type. Field Code Changed Formatted: Font: 11 pt Formatted: Space After: 0 pt, Line spacing: single OSO/IEC 2022 - All rights reserved 7 OSO/IEC 2023 - All rights reserved 	Given two valid signatures $\sigma \underline{\sigma} = (\overline{T_1}, T_1, \overline{T_2}, \overline{T_2}, \overline{J, R, T, c_m}, \overline{F_1}, \overline{T_2}, \overline{T_2}, \overline{J, R, T, c_m}, \overline{F_1}, \overline{T_2}, $	$\rightarrow J, R, T, c_m, \rho$) and $\frac{\hat{\sigma} \hat{\sigma}}{\hat{\sigma}} = (\hat{T}_1 \hat{T}_1, \hat{T}_2)$		Field Code Changed	
 a) If J = J = J and T = = T J, output 1 (linked), otherwise, output 0 (not linked). NOTE If the linking process outputs 0 because of J ≠ ∓ J = J , it means that the linking process cannot determine whether two signatures were created by the same group member. 6.6.6 Revocation process Details of the revocation process in this mechanism are surveyed in Reference [10]. There are two types of revocation process in this mechanism are surveyed in Reference [10]. There are two types of revocation can be either global revocation. Verifier blacklist revocation is a local revocation. Private key revocation: If a group member signature key (+ s, T₁ T₁, T₂ T₂) is compromised, the group membership issue puts + s into a revocation list RL of this type. Field Code Changed Formatted: Font: 11 pt Formatted: Space After: 0 pt, Line spacing: single OSO/IEC 2022 - All rights reserved 7 OSO/IEC 2023 - All rights reserved 	$\hat{T}_2^{'}$, $\frac{\hat{J},\hat{R},\hat{T},\hat{c}_m,\hat{\rho}}{\hat{J}},\hat{R},\hat{T},\hat{c}_m,\hat{\rho}$), the linking process takes the following	lowing steps: 3/PRF Amd 2			
NOTE If the linking process outputs 0 because of $J \neq \hat{\tau} \hat{f} \int \hat{\tau} \hat{f}$, it means that the linking process cannot determine whether two signatures were created by the same group member. 6.6.6 Revocation process Details of the revocation process in this mechanism are surveyed in Reference [10]. There are two types of revocation (private key revocation and verifier blacklist revocation) supported in this mechanism. Private key revocation can be either global revocation or local revocation. Verifier blacklist revocation is a local revocation. Private key revocation is a private key ($\pm s$, $\pm_T T_1$, $\pm_T T_2$) is compromised, the group membership issue puts $\pm s$ into a revocation list RL of this type. Formatted: Font: 11 pt Formatted: Space After: 0 pt, Line spacing: single OSO/IEC 2022 - All rights reserved 7			a0e0-	Field Code Changed	
Details of the revocation process in this mechanism are surveyed in Reference [10]. There are two types of revocation (private key revocation and verifier blacklist revocation) supported in this mechanism. Private key revocation can be either global revocation or local revocation. Verifier blacklist revocation is a local revocation. Private key revocation: If a group member signature key (+s, T₁T₁, T₂T₂) is compromised, the group membership issuer puts +s into a revocation list RL of this type. Formatted: Font: 11 pt Formatted: Space After: 0 pt, Line spacing: single ISO/IEC 2022 - All rights reserved 7 © ISO/IEC 2023 - All rights reserved	NOTE If the linking process outputs 0 because of $J \neq \hat{J} \neq \hat{J}$	it means that the linking process canno	t	Field Code Changed	
of revocation (private key revocation and verifier blacklist revocation) supported in this mechanism. Private key revocation can be either global revocation or local revocation. Verifier blacklist revocation is a local revocation: Private key revocation: — If a group member signature key ($\pm s$, $T_{T}T_{1}$, $T_{Z}T_{2}$) is compromised, the group membership issuer puts $\pm s$ into a revocation list RL of this type. Formatted: Font: 11 pt Formatted: Space After: 0 pt, Line spacing: single Formatted: Space After: 0 pt, Line spacing: single	- 6.6.6 Revocation process				
If a group member signature key (<i>s</i> . <i>s</i> , <i>T</i> ₁ , <i>T</i> ₂ , <i>T</i> ₂) is compromised, the group membership issuer puts <i>s</i> . <i>s</i> into a revocation list RL of this type. Formatted: Font: 11 pt Formatted: Space After: 0 pt, Line spacing: single © ISO/IEC 2022 - All rights reserved 7 © ISO/IEC 2023 - All rights reserved	of revocation (private key revocation and verifier blacklist rev Private key revocation can be either global revocation or local re	vocation) supported in this mechanism	ı.		
puts <u>s S</u> into a revocation list RL of this type. Formatted: Font: 11 pt Formatted: Space After: 0 pt, Line spacing: single So/IEC 2022 - All rights reserved 7 So ISO/IEC 2023 - All rights reserved	Private key revocation:				
© ISO/IEC 2023 – All rights reserved 7 © ISO/IEC 2023 – All rights reserved 7		promised, the group membership issue	r	Field Code Changed	
© ISO/IEC 2023 – All rights reserved 7 © ISO/IEC 2023 – All rights reserved 7	puts $\frac{s}{s}$ into a revocation list RL of this type.				
© ISO/IEC 2022 - All rights reserved 7 © ISO/IEC 2023 - All rights reserved 7				Formatted: Font: 11 pt	
© ISO/IEC 2023 – All rights reserved 7				Formatted: Space After: 0 pt, Line spacing: sin	gle
	© ISO/IEC 2022 – All rights reserved 7				
Orange Restricted	© ISO/IEC 2023 – All rights reserved				
	Orange Restricted		-		

- Given a valid signature $\underline{\sigma} = (\underline{T_1}, \underline{T_1}, \underline{T_2}, \underline{J}, R, T, c_m, \rho)$ computed using a linking base <u>bsn bsn</u> and a revocation list RL of this type, a verifier can check revocation of this signature as follows: for each $\underline{s' \in \text{RL}}$, verify $\underline{T} = [\underline{s'}] \underline{J}$, $\underline{s' \in \text{RL}}$, verify $\underline{T} = [\underline{s'}] \underline{J}$. If any of these verifications fails, output 0 (revoked), otherwise, output 1 (valid).

NOTE 1 The private key revocation works only if the group membership issuer or the verifier has learned the group member signature keys of the compromised group members. This revocation process allows to identify every group signature generated using this private key. If this key can be associated with a group member (e.g. by using contextual information), then no anonymity can be retained for this group member as their-signatures can therefore be traced. This is a property inherent to DAA schemes. Thus, a careful assessment of the need for revocation and the consequences for the corresponding group member will

be carried out before deployment.

Verifier blacklist revocation:

- If signatures were computed using a linking base <u>bsn</u>, a verifier can build its own revocation list RL corresponding to <u>bsn</u>. If the verifier wants to blacklist the signer of a valid signature $\underline{\sigma} = (\underline{\tau}_1, \underline{\tau}_1, \underline{\tau}_2, \underline{\tau}_2, \underline{J, R, T, c_m, \rho}, R, T, c_m, \rho)$, they put $\underline{\tau} \underline{T}$ into a revocation list RL of this type.
- Given a signature $\underline{\sigma} = (\underline{T}_1, \underline{T}_2, \underline{T}_2, \underline{J}, R, T, c_m, \rho)$ computed using a linking base <u>bsn</u> and a revocation list RL of this type, a verifier can check revocation of this signature as follows: for each $\hat{T} - \underline{RL}$, verify $\underline{T} - \underline{\hat{T}} - \underline{$

NOTE 2-In order to use verifier blacklist revocation in this mechanism, a signer must use a specific linking base for each verifier. The value of the linking base can, for example, be chosen by the verifier or agreed in advance by the signer and verifier.

ec-20008-2-2013-prf-amd-

7.1

Replace the first sentence with the following:

This clause specifies three digital signature mechanisms with opening capability.

Replace the text of NOTE with the following:

The mechanisms and associated security proofs in 7.2, 7.3 and 7.4 are based on References-[17], [14] and [23] (the fullan extended version of Reference [24]), respectively.

7.4

Add new subclause 7.4 as follows:

7.4 Mechanism 9

7.4.1 Symbols

8 © ISO/IEC 2022 – All rights reserved

8

© ISO/IEC 2023 – All rights reserved

Orange Restricted

Field Code Changed Field Code Changed Field Code Changed **Field Code Changed** Field Code Changed **Field Code Changed Field Code Changed** Field Code Changed Field Code Changed Field Code Changed Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: Not at 19.85 pt + 39.7 pt + 59.55 pt + 79.4 pt + 99.25 pt + 119.05 pt + 138.9 pt + 158.75 pt + 178.6 pt + 198.45 pt **Field Code Changed Field Code Changed Field Code Changed Field Code Changed** Field Code Changed **Field Code Changed** Field Code Changed **Field Code Changed** Field Code Changed Formatted

Formatted: Default Paragraph Font, Font: Not Bold				
Formatted: Font: 11 pt				
Formatted: Space After: 0 pt, Line spacing: single				

The following symbols apply in the specification of this mechanism.

- $P_{1}P_{1}, S_{1}S_{i}, T_{1}T_{1}, T_{2}K, K', T_{1}T_{2}T_{2}, K, K', T_{1}T_{2}T_{2}$ elements of $G_{1}G_{1}$.
- $= \underbrace{P_2 P_2}_{X,Y,A,B,Y_i,C_1,C_2,C_3,C_4,K_1,K_2,K_3,K_4,K_1,K_2,K_3,K_4,K_1,K_2,K_3,K_4,K_1,K_2,K_3,K_4,K_1,K_2,K_3,K_4}_{X,Y,A,B,Y_i,C_1,C_2,C_3,C_4,K_1,K_2,K_3,K_4,K_1,K_2,K_3,K_4} : elements of \underbrace{G_2 G_2}_{G_2}.$

- $W, W', R, R_T W, W', R, R_i$: elements of $G_T \cdot G_T$.

- $\frac{x, y, a, b, s_i, u, v, k_s, k_u, k_v, c, z_s, z_u, z_v, c', r, t, w, c_m, z, c_m}{x, y, a, b, s_i, u, v, k_s, k_u, k_v, c, z_s, z_u, z_v, c', r, t, w, c_m, z, c_m'}$
- H H: a hash function that outputs elements in $\frac{Z_p}{Z_p} Z_p$.

7.4.2 Key generation process

The group membership issuer key generation process takes the following steps:

- a) Choose a bilinear group pair $(G_{\Gamma}, G_1, G_2, G_2)$ of large prime order $p \cdot p$, such that no efficiently computable homomorphism is known between G_{Γ}, G_1 and G_2, G_2 , in either direction, and an associated pairing function $e \cdot e : G_{\Gamma}, G_1 \times G_2, G_2 \to G_T, G_T$.
- b) Choose a random generator $P_{T_1}P_1$ of $G_{T_1}G_1$ and a random generator $P_{Z_1}P_2$ of $G_{Z_2}G_2$. And 2 c) Choose two random integers $\frac{x}{x}$ and $\frac{y}{y}$ in $\frac{Z_p}{Z_p}Z_p$.

d) Compute $X = [x]P_2$ and $Y = [y]P_2$.

```
d) Compute X = [x]P_2 and Y = [y]P_2.
```

- e) Choose a hash function $H H: \{0,1\}^* \{0,1\}^* \to Z_p$. An example of how to construct such Z_p . Such a hash function is provided shall be constructed as described in Annex B.
- f) Output the following:
 - group public parameters: $(\underline{G_1}, \underline{G_2}, \underline{G_2}, \underline{G_T}, \underline{G_T}, \underline{e}, \underline{p}, \underline{p}, \underline{H}, \underline{P_1}, \underline{P_2}, \underline{H}, \underline{P_1}, \underline{P_2})$
 - group public key: (X, Y, X, Y),
 - group membership issuing key: (<u>x, y</u> x, y).

© ISO/IEC 2022 – All rights reserved 9

© ISO/IEC 2023 – All rights reserved

Orange Restricted

	Formatted	
A	Field Code Changed	
11	Field Code Changed	<u></u>
1	Field Code Changed	
-	Field Code Changed)
	Field Code Changed	
	Field Code Changed	
_	Field Code Changed	
1	Field Code Changed	
Å	Field Code Changed	
1	Field Code Changed	
1	Field Code Changed	
/ //	Field Code Changed	
	Field Code Changed	$\vec{\Box}$
	Field Code Changed	لي
	Field Code Changed	in the second se
	Field Code Changed	
	Field Code Changed	
	Field Code Changed	
	Field Code Changed	Ē
1/1	Field Code Changed	
1/1	Field Code Changed	
1/1	Field Code Changed	
1	Field Code Changed	
1	Field Code Changed 1/1000	Ē
1	Field Code Changed	
11	Field Code Changed	
	Field Code Changed	
1	Field Code Changed	Ĩ
_	Field Code Changed	Ē
1	Field Code Changed	Ĩ
_	Field Code Changed	
-	Field Code Changed	Ē
1	Field Code Changed	Ĩ
1	Field Code Changed	Ĩ
	Field Code Changed	Ē
-	Field Code Changed	Ĩ
Y	Field Code Changed	Ē
1	Field Code Changed	Ē
1	Formatted	Ē
1	Formatted	H
		ر
11		

L