..... I

..... II

..... 1

1. 1
2. 2
3. 3
4. 3
5. 5
6. 6
7. 7
8. 7

..... 8

..... 8

9. 8
10. 10

..... 10

11. 10
12. 14
13. 14

..... 15

14. 15
15. 15
16. 16
17. 18
18. 19

..... 20

19. 20
20. 21
21. 22
22. 23

..... 29

23. 29
24. 30

..... 31

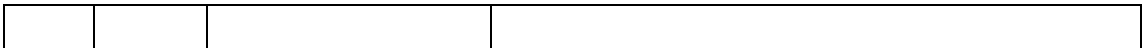
25. 31
26. 31
27. 32

..... 33

28. 2023 D 33

. 34
29. 34
30. 34
31. 35
32. 36
. 36
33. 36
34. 37
35. 42
36. 43
. 44
. 44

mplwh@cacrnet.org.cn



29	26		15.2
30	27		
31	28		
32	30		
33	31		
34	32		
35	34.1		/
36	34.2		
37	36		

1.

GB/T 39786-2021

GB/T 22239

1.1

GB/T 39786-2021

GB/T 22240-2020

GB/T 39786-2021

GB/T 39786-2021

1.2

GB/T 39786-2021

1.3

GB/T 39786-2021

GB/T 39786-2021

GB/T 39786-2021

2.

GB/T 39786 “ ” “ ” “ ”

”

3.

39 2020 7 1 ,

2020 6 30

“ ”

4.

GM/T 0115 “ 5.2
” / “ 5.3
”

4.1

4.2

VPN

-

-

bug

SSL VPN

SSL VPN

SSL

-

4.3

GM/T 0018-2012

GM/T 0029 GM/T 0028

4.4

“ 5.2 ” “ ”

“ ”

“ ”

1 GB/T 39786 GB/T 39786 GB/T 37092

2

3

/ /

4

5.

GB/T 39786 8.4 “ d)
e)
f)
g)
”

GB/T 39786-2021
GM/T 0115-2021

“ ”

“ ”

6.

DES SM4 DES
SM4(DES(data))

“ ”

DAK

7.

8.

9.

GB/T 39786 8.1 “ a)

b) c)

” GM/T 0115

“ 6.1 ”

9.1

1

IDC

“ ” “ ”

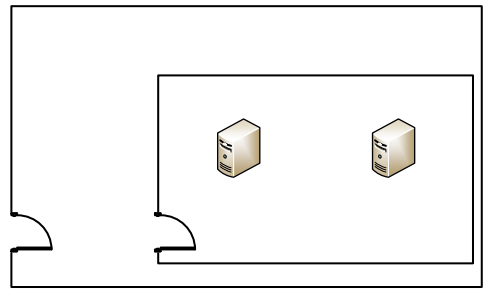
“ ”

2 IDC

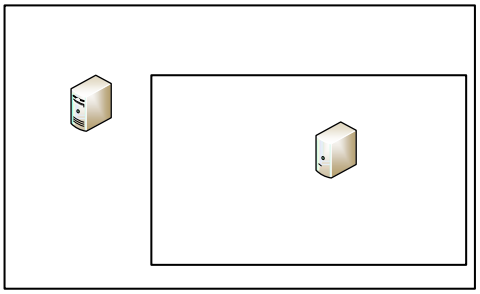
“ ”

IDC

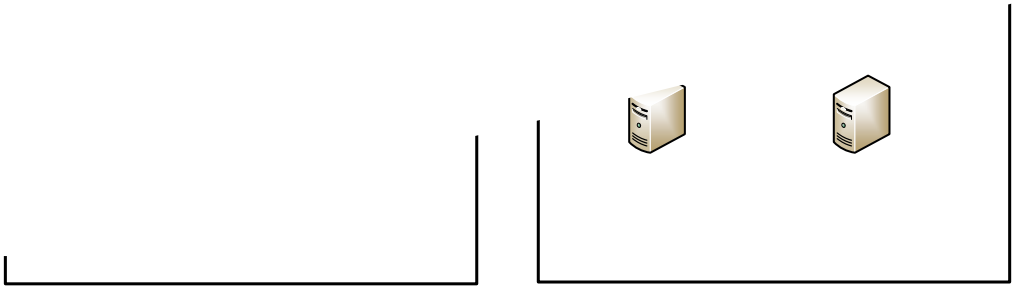
9.2



9-1



9-2



9-3

➢ 9-1

1 2

2

- 9-2 1
- 9-3 1 2

10.

GM/T 0036-2014

GM/T 0036

11.

GB/T 39786

11.1

1

2

PC web

APP

IPSec VPN IPSec VPN

(1)

HTTPS

(2) VPN SSL VPN

HTTPS

(3) SSL VPN

(4) IPSec VPN

			SSL VPN	SSL VPN	IPSec VPN
			-	-	-
		-	-	-	-
VPN	-	-			-
IPSec VPN	-	-	-	-	

k Ŏ Ç ˆ Ç

1		HTTPS HTTPS
2		HTTPS HTTPS
3		HTTPS HTTPS
4		HTTPS HTTPS
5	VPN SSL VPN	SSL VPN SSL VPN
6		HTTPS HTTPS
7	VPN SSL VPN	SSL VPN SSL VPN
8	IPSec VPN IPSec VPN	IPSec VPN IPSec VPN

11.2

“

”

11.3

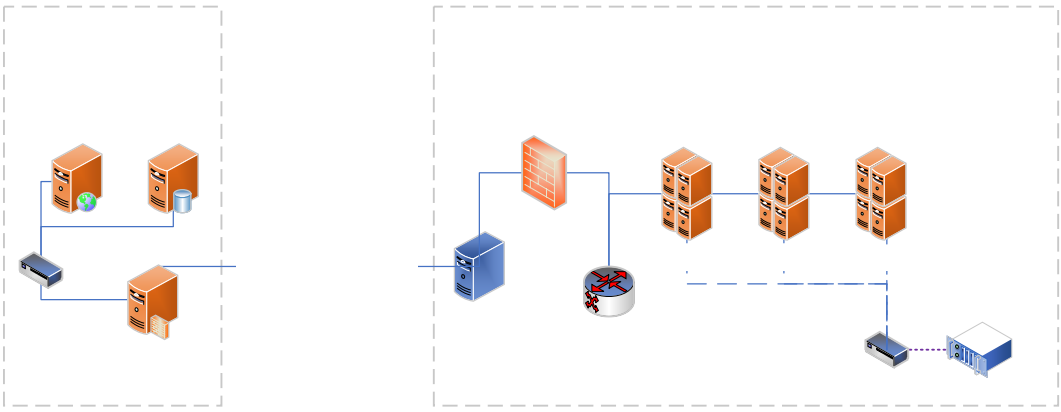
11.4

GM/T 0115

11.5

“ ”

11-1



11-1

“ ” “ ”

12.

SSL VPN

SSL VPN

SSL VPN

“ ”

“ ”

D A K D A × K

“ ”

D A K D

A × K ×

13.

GB/T 39786-2021 8.2

e)

“

”

“ ”

IPSec VPN SSL /

IPSec VPN SSL “

”

“ ” “ ”

“ ”

14.

GM/T 0115

WAF

/

15.

IPSec VPN

“ ”

/

5 A B

C 3 D E

F

“ ” “ A-B- C

D-E-F ”

D/A/K

IPSec VPN SSL VPN

“

”

5

GMxxx IPSec VPN

“ ” “ IPSec VPN

GMxxx ”

D/A/K

16.

16.1

“ ”

“ ”

ضخ ; c Ş

“ ”

“ ”

16.2

+

(1) “

” “ ”

Ş Ş . z B A

MAC

17.

GM/T 0115

“

” “ ”

“ ”

“ ”

SSL VPN

“

”

SSL VPN

VPN

“ ”

VPN

HTTPS

SSH

SSL

VPN ţ

/

SSL VPN

“ ”

18.

“ ” “ ” “

” “ ”

/

“ ” “

” “ ”

/

“ ”

IC

IC

“ ” “

” “ ”

“ ” “ ”

“ ”

19.

GM/T 0115

“ ”

19.1

19.2

/

19.3

19.4

“ ” “

” “ ”

20.

“ ”

“ ” “ ”

“ ”

“ ”

21.

GB/T 39786-2021

21.1

SM3

SM3

SM3

HMAC-SM3 SM4 MAC

GB/T15852.1-2020

21.2

SM4-ECB

ECB

ECB

22.

2023 3.3.2 “
” 4 “ ” A.4 “ ”
4 “ ”

3.3.2.1 “ 3-7
” 4 “ 4-4
”

4 “ 4-4
”

OA

OA

OA

3.3.2.1 “ 3-7 ”

3-7

1		☑ ☑ ☑ ☑ ☑	

4 “ ” 4-4

4-4

		符合/部分符合/不符合/不适用							
1									
/ / /									

4-5

4-5

1	OA	
2	OA	
3		
4		
/ / /		

4-6

4-6

1	OA				
2	OA				
3	OA				
4	OA				
5	OA				
6					
7					
8					
9					
/ / /					

4-7

4-7

1	OA	
2		
/ / /		

A-4

A-4

			D	

						1	
						1	
	OA			×	×	0.25	
						1	
	OA					/	
						/	
	OA		×	/	/	0	
	OA		×	/	/	0	
	OA					/	
	OA					/	
	OA					/	

						1	
	OA					1	
	OA					1	
	OA					/	
	OA					/	
	OA					/	
						1	
						1	
						1	
						1	
	OA		×	/	/	0	
	OA		×	/	/	0	

	OA					1	
	OA					1	
	OA					1	
				/	/	0	
			×	/	/	0	
			×	/	/	0	
			×	/	/	0	
	OA		×	/	/	0	
	OA		×		/	0	
	OA					1	
	OA					1	
	OA					1	

			×	/	/	0	
						1	
						1	
	OA						
				×		0.5	

“

”

VPN

“

”

“

24.

GM/T 0115-2021

“

”

“ ” “ ”

“ ” “ ”

K /

25.

GB/T 39786 2021 9.7 a)
“ ”

GB/T 39786 2021 9.7 a)

GM/T 0115

GM/T 0115

26.

GB/T 39786-2021 8.7 d)
“ ”

“

”

“ ”

1 2020 1 1

“ ”

2 2020 1 1

“ ”

“ ” “ ”

GB/T 39786

“ ”

/

27.

/ SSH

GB/T 39786-2021

GM/T 0115-2021

“ ”

“ ”

28. 2023 D

GB/T 39786-2021 8.4
“ d) e)
f)
g)
”

MD5

DES MD5
D

/ “ D ”
2023

- 112 3DES 3
AES-128 SHA-224 RSA-2048 ECDSA-P224
- 80 112 RSA-1024
3DES 2 ECDSA-P192

- 80 DES MD5 SHA-1 RSA-512

29.

1

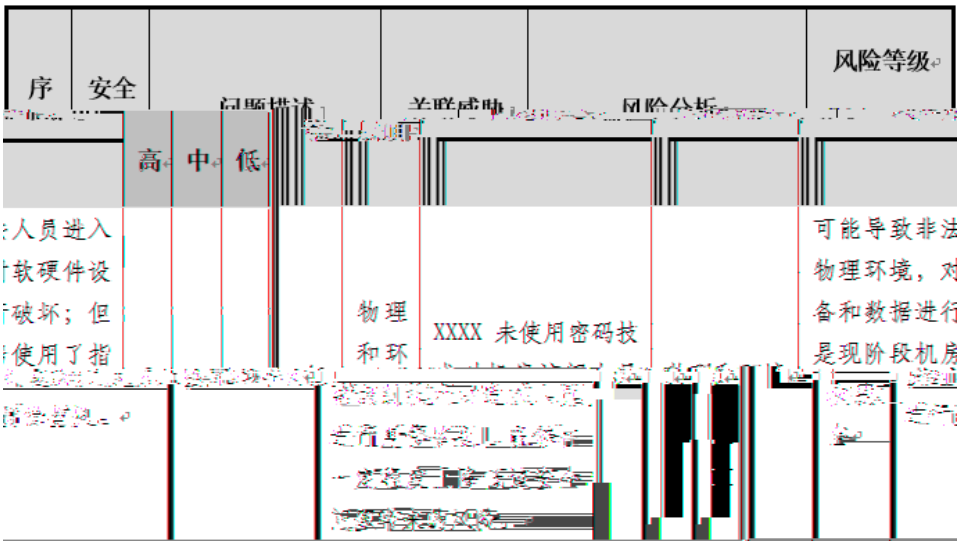
,

A

2023 “

” 6-1

表 6-1 风险分析



31.

“ ” “ ” “ ”

“ ”

“ ” “ ”

“ ” “ ”

“ ” “ ”

2023 5.1

“ ”

“ ”

“ ” “ ”

“ ” “ ”

“ ” “ ”

“ ” “ ”

“ ” “ ”

“ ”

32.

“ ”

1 “ ”

2 “ ”

1 “ ” “
”

2

34.

GB/T 39786-2021

34.1

2

“ ”

3

1 “ ” “ ”

“

”

2 “ ” ”

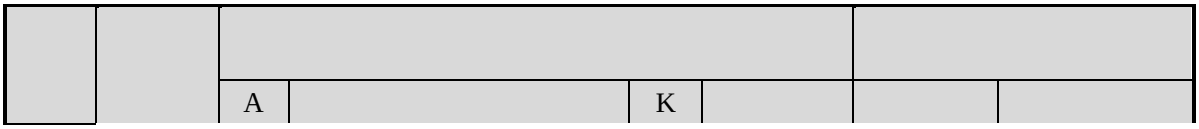
”

34-1

1				1		/
2				0.5		
3				0.5		
4				0.5		
5				1		/
6				1		/
7				1		/
8		……	……	……	……	……
9				1		/
10				1		/
11				0.25		
12				0		
13		……	……	……	……	……
14				0.5		

15		……	……	……	……	……

34-2



SM3 SM2

“ ” ……

1

“ ” “

” “ ”

36.

1	1.1	1
2	1.2	/
3	1.3	/
4	2	2
5	3	17
6	4.1	16
7	4.2	/
8	4.3	/
9	4.4	3
10	5	13
11	6	/
12	7	/
13	8	/
14	9.1	4
15	9.2	/
16	10	9.2
17	11.1	5.1
18	11.2	5.2
19	11.3	5.3
20	11.4	20
21	11.5	/
22	12	/
23	13	25
24	14	6
25	15	7
26	16.1	10.1
27	16.2	10.2 10.3
28	17	8
29	18	9.1
30	19.1	11.1
31	19.2	11.2
32	19.3	/
33	19.4	/
34	20	/
35	21.1	12
36	21.2	/
37	22	24

38	23	14
39	24	/
40	25	15.1
41	26	15.2
42	27	/
43	28	/
44	29	18
45	30	19
46	31	26
47	32	/
48	33	21
49	34.1	22
50	34.2	/
51	35	23
52	36	/