QUALIFICATION FILE – Standalone NOS

Essentials of Data Encryption and Cryptographic Security

☐ Horizontal/Generic ☐ Vertical/Specialization

☐ Upskilling ☐ Dual/Flexi Qualification ☐ For ToT ☐ For ToA

☐General ☐ Multi-skill (MS) ☐ Cross Sectoral (CS) ☒ Future Skills ☐ OEM

NCrF/NSQF Level: 5

Submitted By:

National Institute of Electronics and Information Technology

NIELIT Bhawan,
Plot No. 3, PSP Pocket, Sector-8,
Dwarka, New Delhi-110077,
Phone: - 91-11-2530 8300
e-mail: - contact@nielit.gov.in

Table of Contents

Section 1: Basic Details

1.	**NOS-Qualification Name**	**Essentials of Data Encryption and Cryptographic Security**	
2.	**Sector/s**	IT-ITeS	
3.	**Type of Qualification ☒ New ☐ Revised**	**NQR Code & version of the existing /previous qualification: NA**	**Qualification Name of the existing/previous version: NA**
4.	**National Qualification Register (NQR) Code & Version** *(Will be issued after NSQC approval.)*	NG-05-IT-04175-2025-V1-NIELIT	**5. NCrF/NSQF Level: 5**
6.	**Brief Description of the Standalone NOS**	The "**Essentials of Data Encryption and Cryptographic Security**" course provides an in-depth understanding of encryption techniques essential for modern cybersecurity. It covers the fundamentals of encryption, including symmetric (AES, DES, 3DES) and asymmetric encryption (RSA, ECC), digital signatures, and key management strategies. Additionally, students explore steganography, public key infrastructure (PKI), and real-world applications of cryptographic security. Hands-on labs involve implementing encryption algorithms using Python, OpenSSL, and GPG, ensuring practical proficiency. The course culminates in projects on secure communications and key management, equipping students with the necessary skills for data security in diverse applications.	
7.	**Eligibility Criteria for Entry for a Student/Trainee/Learner/Employee**	**a. Entry Qualification & Relevant Experience:**	

S. No.	Academic/Skill Qualification (with Specialization - if applicable)	Required Experience (with Specialization - if applicable)
1	UG Diploma	NA
2	2nd year of UG in CS/IT/EC/EE/ allied branches	NA
3	2nd year of diploma in CS/IT/EC/EE/ allied branches (after 12th)	NA
4	3-year Diploma in CS/IT/EC/EE/ allied branches after 10th	1.5 years experience in cyber security and allied subsector of IT
5	Previous relevant Qualification of NSQF Level 4.5	1.5 years experience in cyber security and allied subsector of IT

<table>
<tr><td><b>8.</b></td><td><b>Credits Assigned to this NOS-Qualification, Subject to Assessment</b> <i>(as per National Credit Framework (NCrF))</i></td><td><b>4 Credits</b></td><td><b>9.</b></td><td><b>Common Cost Norm Category (I/II/III)</b> <i>(wherever applicable)</i>:
<b>Category-II</b></td></tr>
<tr><td><b>10.</b></td><td><b>Any Licensing Requirements for Undertaking Training on This Qualification</b> <i>(wherever applicable)</i></td><td colspan="3">No</td></tr>
<tr><td><b>11.</b></td><td><b>Training Duration by Modes of Training Delivery</b> <i>(Specify <b>Total Duration</b> as per selected training delivery modes and as per requirement of the qualification)</i></td><td colspan="3"><b>☒Offline ☐Online ☐Blended</b>
<table>
<tr><th>Training Delivery Modes</th><th>Theory (Hours)</th><th>Practical (Hours)</th><th>Total (Hours)</th></tr>
<tr><td><b>Classroom (offline)</b></td><td>45</td><td>75</td><td>120</td></tr>
</table></td></tr>
<tr><td><b>12.</b></td><td><b>Assessment Criteria</b></td><td colspan="3">
<table>
<tr><th>Theory (Marks)</th><th>Practical (Marks)</th><th>Project/Presentation/ Assignment (Marks)</th><th>Viva/Internal Assessment (Marks)</th><th>Total (Marks)</th><th>Passing %age</th></tr>
<tr><td>100</td><td>60</td><td>20</td><td>20</td><td>200</td><td>50</td></tr>
</table>
The centralised online assessment is conducted by the Examination Wing, NIELIT Headquarters.
*Assessment strategy shall be as per NIELIT Norms prevailing at times.</td></tr>
<tr><td><b>13.</b></td><td><b>Is the NOS Amenable to Persons with Disability</b></td><td colspan="3"><b>☒ Yes ☐ No If “Yes”, specify applicable type of Disability:</b>
a. Locomotor Disability
● Leprosy Cured Person
● Dwarfism
● Muscular Dystrophy
● iv. Acid Attack Victims
b. Visual Impairment
c. Low Vision</td></tr>
<tr><td><b>14.</b></td><td><b>Progression Path After Attaining the Qualification, wherever applicable</b> <i>(Please show Professional and Academic progression)</i></td><td colspan="3">Cryptography Engineer</td></tr>
</table>

15.	**How participation of women will be encouraged?**	Participation by women can be ensured through Government Schemes. Occasionally, exclusive batches for women would be run for the proposed courses. Funding is available for women's participation under other schemes launched by the Government from time to time.	
16.	**Other Indian languages in which the Qualification & Model Curriculum are being submitted**	Qualification file available in English & Hindi Language.	
17.	**Is similar NOS available on NQR-if yes, justification for this qualification**	**☐ Yes ☒ No URLs of similar Qualifications:**	
18.	**Name and Contact Details Submitting / Awarding Body SPOC** *(In case of CS or MS, provide details of both Lead AB & Supporting ABs)*	**Name:** Shri Niladri Das **Email:** niladridas@nielit.gov.in **Contact No.:** 8794028299 **Website:** https://nielit.gov.in/index.php	
19.	**Final Approval Date by NSQC: 08.05.2025**	**20. Validity Duration: 3 Years**	**21. Next Review Date: 08.05.2028**

Section 2: Training Related

1.	**Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	A-Level/MCA/ B. Tech in CS/IT/M.Sc(IT/CS) allied areas with 1 years of Experience in training.
2.	**Master Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	A-Level/MCA/ B. Tech in CS/IT/M.Sc(IT/CS) allied areas with 2 years of Experience in training.
3.	**Tools and Equipment Required for the Training**	☒Yes ☐No (If "Yes", details to be provided in Annexure)
4.	**In Case of Revised NOS, details of Any Upskilling Required for Trainer**	NA

Section 3: Assessment Related

1.	**Assessor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	A-Level/MCA/ B. Tech in CS/IT/M.Sc(IT/CS) allied areas with 2 years of Experience in training.
2.	**Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines), (wherever applicable)*	The assessor carries out theory online assessments through the remote proctoring methodology. Theory examination would be conducted online, and the paper comprise of MCQ. Conduct of assessment is through trained proctors. Once the test begins, remote proctors have full access to the candidate's video feeds and computer screens. Proctors authenticate the candidate based on registration details, pre-test image captured and I- card in possession of the candidate. Proctors can chat with candidates or give warnings to candidates. Proctors can also take screenshots, terminate a specific user's test session, or re-authenticate candidates based on video feeds.
3.	**Lead Assessor's/Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	External Examiners/ Observers (Subject matter experts) are deployed including NIELIT scientific officers who are subject experts for evaluation of Practical examination/ internal assessment / Project/Presentation/ assignment and Major Project (if applicable). Qualification is generally B.Tech.
4.	**Assessment Mode** *(Specify the assessment mode)*	Centralized online examination will be conducted
5.	**Tools and Equipment Required for Assessment**	☒ Same as for training ☐ Yes ☐ No (details to be provided in Annexure-if it is different for Assessment)

Section 4: Evidence of the Need for the Standalone NOS

Provide Annexure/Supporting documents name.

1.	Government /Industry initiatives/ requirement (Yes/No): Yes, Available at Annexure-A: Evidence of Need
2.	Number of Industry validation provided: 3
3.	Estimated number of people to be trained: 500
4.	Evidence of Concurrence/Consultation with Line/State Departments (In case of regulated sectors): (Yes/No): NIELIT is recognized as AB and AA under Government Category. NIELIT is an HRD arm of MeitY, therefore, the Line Ministry Concurrence is not required.

Section 5: Annexure & Supporting Documents Check List

Specify Annexure Name / Supporting document file name

1.	**Annexure:** NCrF/NSQF level justification based on NCrF/NSQF descriptors *(Mandatory)*	Available at Annexure-I: Evidence of Level
2.	**Annexure:** List of tools and equipment relevant for NOS *(Mandatory, except in case of online course)*	Available at Annexure-II: Tools and Equipment
3.	**Annexure:** Industry Validation	Available at Annexure-III: Industry Validation
4.	**Annexure:** Training Details	Available at Annexure-IV: Training Details
5.	**Annexure:** Blended Learning *(Mandatory, in case selected Mode of delivery is "Blended Learning")*	Available at Annexure-V: Blended Learning
6.	**Annexure/Supporting Document:** Standalone NOS- Performance Criteria Details Annexure/Document with PC-wise detailing as per NOS format (Mandatory- Public view)	Available at Annexure-VI: Standalone NOS- Performance Criteria details
7.	**Annexure:** Detailed Assessment Criteria *(Mandatory)*	Available at Annexure-VII: Assessment Criteria
8.	**Annexure:** Assessment Strategy *(Mandatory)*	Available at Annexure-VIII: Assessment Strategy
9.	**Annexure:** Acronym and Glossary *(Optional)*	Available at Annexure-IX: Acronym and Glossary
10.	**Supporting Document:** Model Curriculum *(Mandatory – Public view)*	Available at Annexure-B Model Curriculum

Annexure-I: Evidence of Level

NCrF/NSQF Level Descriptors	Key requirements of the job role/ outcome of the qualification	How the job role/ outcomes relate to the NCrF/NSQF level descriptor	NCrF/NSQF Level
Professional Theoretical Knowledge/Process	The "Essentials of Data Encryption and Cryptographic Security" course equips learners with both professional skills and theoretical knowledge essential for cybersecurity roles such as Cryptography Engineer, Cybersecurity Analyst, and Network Security Engineer. Graduates gain expertise in symmetric and asymmetric encryption (AES, RSA, ECC), cryptographic protocols (SSL/TLS, IPSec), key management, and data privacy compliance (GDPR, HIPAA, PCI-DSS). They develop practical skills in implementing encryption algorithms using Python and OpenSSL, securing communications, configuring Public Key Infrastructure (PKI), and analyzing cryptographic vulnerabilities. The course also covers cryptographic attacks, digital forensics, and post-quantum cryptography, ensuring readiness for professional certification and further academic progression.	The job role and outcomes align with aligning with NSQF Level 6 or 7, this course ensures that learners achieve a blend of technical mastery, professional competencies, and problem-solving skills, making them employment-ready professionals and potential cybersecurity entrepreneurs. It provides a pathway for career growth, industry certification, and further academic progression, supporting roles in network security, cryptography, penetration testing, and compliance management.	5
Professional and Technical Skills/ Expertise/ Professional Knowledge	The qualification will develop a strong foundation in professional knowledge, technical skills, and expertise required for securing sensitive data and digital communications. They will gain expertise in encryption methodologies, including symmetric (AES, DES, 3DES) and asymmetric (RSA, ECC) encryption, along with hash functions (SHA-256, MD5) for data integrity. Their proficiency in key management, digital signatures, and cryptographic protocols such as SSL/TLS, VPN, and PKI ensures secure data transmission and authentication. Additionally, they will acquire practical skills in cryptographic attack prevention, penetration testing, and vulnerability assessment, allowing them to identify and mitigate security risks such as brute-force attacks, side-channel attacks, and man-in-the-middle threats. With hands-on experience in steganography, secure key storage, digital forensics, and compliance frameworks, graduates will be prepared to implement robust security solutions.	Factual knowledge of field of knowledge or study.	5
Employment Readiness & Entrepreneurship	This qualification prepares employment-ready with a strong professional skill set, entrepreneurial mindset, and cybersecurity expertise essential for success in the digital security domain. They will possess hands-on experience in implementing encryption algorithms, managing cryptographic keys, securing network communications, and conducting risk assessments,	Recall and demonstrate practical skill, routine and repetitive in narrow range of application, using appropriate rule and tool, using quality concepts	5

Skills & Mind-set/Professional Skill	making them highly valuable for roles such as Cryptography Engineer, Cybersecurity Analyst, and Security Consultant. Their ability to analyze vulnerabilities, mitigate threats, and ensure regulatory compliance (GDPR, HIPAA, PCI-DSS) enhances their employability in industries like finance, healthcare, and cloud computing. Beyond technical proficiency, graduates will develop critical thinking, problem-solving, and ethical decision-making skills, fostering a security-first mindset essential in today's cybersecurity landscape. For those with an entrepreneurial drive, expertise in data protection, encryption-based product development, and cybersecurity consultancy will enable them to launch their own ventures, offering customized encryption solutions, security audits, and compliance advisory services. Their adaptability, communication skills, and innovative approach to cybersecurity challenges will make them both industry-ready professionals and future cybersecurity entrepreneurs.		
Broad Learning Outcomes/Core Skill	They will be able to handle alone as well as in /with the team in the area as per the curriculum	Language to communicate written or oral, with required clarity, skill to basic arithmetic and algebraic principles, basic understanding of social political and natural environment.	5
Responsibility	This course is designed to equip students with a comprehensive understanding of encryption techniques and their applications in modern cybersecurity. Students will be responsible for mastering fundamental encryption concepts, including symmetric (AES, DES, 3DES) and asymmetric encryption (RSA, ECC), digital signatures, and key management strategies. They will also explore advanced topics such as steganography, public key infrastructure (PKI), and real-world cryptographic security applications	Responsibility for own work and learning.	5

Annexure-II: Tools and Equipment (lab set-up)

List of Tools and Equipment

Batch Size: 30

S. No.	Tool / Equipment Name	Specification	Quantity for specified Batch size
1	Classroom	1 (30 Sq.m)	30
2	Student Chair	-	30
3	Student Table	-	30
4	Desktop computer with accessories	● 12th Generation Intel® Core™ i5-12500T with Intel vPro® Enterprise ● 8 GB DDR4-3200 MHz RAM (1 x 8 GB) ● 512 GB PCIe® NVMe™ M.2 SSD ● Intel® UHD Graphics 770 ● Windows 11 Professional	30
5	Deskjet printer	1 Nos.	A4

Classroom Aids

The aids required to conduct sessions in the classroom are:

1. LCD Projector/Smart Board
2. Pin-up Board
3. White Board, Markers

Annexure-III: Industry Validations Summary

S. No	Organization Name	Representative Name	Designation	Contact Address	Contact Phone No	E-mail ID
1	Tripura University (A Central University)	Prof. Swanirbhar Majumder	Professor, Head of the Department, Department of Information Technology	Tripura University (A Central University) Suryamaninagar, Tripura(W) Pin: 799022	9436229406	hod_it@tripurauniv.ac.in
2	Software World	Amrita Saha	Proprietor	Ujan Abhoynagar, Manipuripara, West Tripura, Pin: 799001	03817963527	support@softwareworld.co.in
3	Trend Micro India Pvt. Ltd.	Kanchan Mallick	Sr. Regional Account	10th floor, EROS Corporate Tower, Nehru Place, New Delhi – 110019	9903003292	

Annexure-IV: Training Details

Training Projections:

Year	Estimated Training # of Total Candidates	Estimated training # of Women	Estimated training # of People with Disability
2025	100	50	10
2026	200	70	15
2027	200	70	15

Data to be provided year-wise for next 3 years.

Annexure-V: Blended Learning

Blended Learning Estimated Ratio & Recommended Tools: NA

Annexure-VI: Performance Criteria details

1. Description:

The "Essentials of Data Encryption and Cryptographic Security" course provides an in-depth understanding of encryption techniques essential for modern cybersecurity. It covers the fundamentals of encryption, including symmetric (AES, DES, 3DES) and asymmetric encryption (RSA, ECC), digital signatures, and key management strategies. Additionally, students explore steganography, public key infrastructure (PKI), and real-world applications of cryptographic security. Hands-on labs involve implementing encryption algorithms using Python, OpenSSL, and GPG, ensuring practical proficiency. The course culminates in projects on secure communications and key management, equipping students with the necessary skills for data security in diverse applications.

2. Scope:

The scope covers the following:

- Covers symmetric encryption (AES, DES, 3DES) and asymmetric encryption (RSA, ECC), along with digital signatures and key management strategies.
- Hands-on experience with encryption algorithms using Python, OpenSSL, and GPG to ensure real-world application of cryptographic security.
- Focuses on secure communication protocols, key management practices, and cryptographic security in diverse applications.

3. Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

Introduction to Data Encryption

PC1. Understand the fundamental concepts of data encryption and its importance in cybersecurity.

PC2. Identify common attacks on encrypted systems and explain possible countermeasures.

PC3. Learners should be able to compare and contrast the types of encryption and explain when each is used.

Symmetric Encryption

PC4. Explain the concept and applications of symmetric encryption

PC5. Demonstrate the implementation of block ciphers (AES, DES, 3DES) and stream ciphers

Asymmetric Encryption

PC6. Demonstrate the ability to perform key generation, encryption, and decryption using the RSA algorithm.

PC7. Explain the principles of Elliptic Curve Cryptography (ECC) and compare its features with symmetric encryption techniques.

Data Privacy and Digital Signature

PC8. Learn about digital signatures, data privacy, and the role of encryption in securing data.

PC9. Explain the importance of data privacy in modern systems and describe key related acts and their salient features.

Key Management

PC10. Demonstrate understanding and application of secure key distribution and storage methods.

PC11. Apply knowledge of hardware security elements (HSMs) in managing cryptographic keys securely.

Steganography

PC12. Understand the concept of Steganography and its uses.

PC13. Demonstrate and differentiate between various steganography techniques, including image, audio, and video steganography.

Public Key Infrastructure (PKI)

PC14. Develop hands-on skills in implementing encryption algorithms and managing encryption keys.

PC15. Demonstrate the process of creating and submitting a Certificate Signing Request (CSR) for digital certificate issuance.

4. Knowledge and Understanding (KU):

The individual on the job needs to know and understand:

KU1. Understanding core encryption principles, including symmetric and asymmetric encryption, digital signatures, and key management techniques.

KU2. Gaining practical knowledge of encryption tools like Python, OpenSSL, and GPG for securing data and communications.

KU3. Understanding how cryptographic security applies to secure communications, public key infrastructure (PKI), and data protection in various industries.

5. Generic Skills (GS):

User/individual on the job needs to know how to:

GS1. Follow instructions, guidelines and procedures

GS2. Listen effectively and communicate information accurately

GS3. Apply formatting features to achieve the desired results

Annexure-VII: Assessment Criteria

Detailed PC-wise assessment criteria and assessment marks for the NOS are as follows:

NOS/Module Name	Assessment Criteria for Performance Criteria	Theory Marks	Practical Marks	Project Marks	Viva Marks
Essentials of Data Encryption and Cryptographic Security **NOS Code: NIE/ITS/N0916**	**Introduction to Data Encryption:** **PC1.** Understand the fundamental concepts of data encryption and its importance in cybersecurity. **PC2.** Identify common attacks on encrypted systems and explain possible countermeasures. **PC3.** Learners should be able to compare and contrast the types of encryption and explain when each is used.	10	5	2	2
	Symmetric Encryption: **PC4.** Explain the concept and applications of symmetric encryption **PC5.** Demonstrate the implementation of block ciphers (AES, DES, 3DES) and stream ciphers	20	10	4	4
	Asymmetric Encryption: **PC6.** Demonstrate the ability to perform key generation, encryption, and decryption using the RSA algorithm. **PC7.** Explain the principles of Elliptic Curve Cryptography (ECC) and compare its features with symmetric encryption techniques.	20	10	4	4
	Data Privacy and Digital Signature: **PC8.** Learn about digital signatures, data privacy, and the role of encryption in securing data. **PC9.** Explain the importance of data privacy in modern systems and describe key related acts and their salient features.	20	10	4	4
	Key Management: **PC10.** Demonstrate understanding and application of secure key distribution and storage methods. **PC11.** Apply knowledge of hardware security elements (HSMs) in managing cryptographic keys securely.	10	10	2	2

	Steganography **PC12.** Understand the concept of Steganography and its uses. **PC13.** Demonstrate and differentiate between various steganography techniques, including image, audio, and video steganography.	10	5	2	2
	Public Key Infrastructure (PKI): **PC14.** Develop hands-on skills in implementing encryption algorithms and managing encryption keys. **PC15.** Demonstrate the process of creating and submitting a Certificate Signing Request (CSR) for digital certificate issuance.	10	10	2	2
Total Marks		**100**	**60**	**20**	**20**

Annexure-VIII: Assessment Strategy

This section includes the processes involved in identifying, gathering, and interpreting information to evaluate the Candidate on the required competencies of the program.

Assessment of the qualification evaluates candidates to ascertain that they can integrate knowledge, skills and values for carrying out relevant tasks as per the defined learning outcomes and assessment criteria.

The underlying principle of assessment is fairness and transparency. The evidence of the outcomes and assessment criteria. competence acquired by the candidate can be obtained by conducting Theory (Online) examination.

About Examination Pattern:

1. The question papers for the theory exams are set by the Examination wing (assessor) of NIELIT HQS.
2. The assessor assigns roll number.
3. The assessor carries out theory online assessments. Theory examination would be conducted online and the paper comprise of MCQ
4. Pass percentage would be 50% marks.
5. The examination will be conducted in English language only.

Quality assurance activities: A pool of questions is created by a subject matter expert and moderated by other SME. Test rules are set beforehand. Random set of questions which are according to syllabus appears which may differ from candidate to candidate. Confidentiality and impartiality are maintained during all the examination and evaluation processes.

Annexure-IX: Acronym and Glossary

Acronym

Acronym	**Description**
AA	Assessment Agency
AB	Awarding Body
NCrF	National Credit Framework
NOS	National Occupational Standard(s)
NQR	National Qualification Register
NSQF	National Skills Qualifications Framework

Glossary

Term	**Description**
National Occupational Standards (NOS)	NOS define the measurable performance outcomes required from an individual engaged in a particular task. They list down what an individual performing that task should know and also do.
Qualification	A formal outcome of an assessment and validation process which is obtained when a competent body determines that an individual has achieved learning outcomes to given standards
Qualification File	A Qualification File is a template designed to capture necessary information of a Qualification from the perspective of NSQF compliance. The Qualification File will be normally submitted by the awarding body for the qualification.
Sector	A grouping of professional activities on the basis of their main economic function, product, service or technology.