1.	Record Nr.	UNINA9910298990503321
	Autore	Pape Sebastian
	Titolo	Authentication in Insecure Environments : Using Visual Cryptography and Non-Transferable Credentials in Practise / / by Sebastian Pape
	Pubbl/distr/stampa	Wiesbaden : , : Springer Fachmedien Wiesbaden : , : Imprint : Springer Vieweg, , 2014
	ISBN	3-658-07116-8
	Edizione	[1st ed. 2014.]
	Descrizione fisica	1 online resource (365 p.)
	Disciplina	004 005.7 005.74
	Soggetti	Data structures (Computer science) Computers Data Structures and Information Theory Information Systems and Communication Service
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Description based upon print version of record.
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Mathematical and Cryptographic Foundation -- Human Decipherable Encryption Schemes: Introduction, Scenario, and Related Work - Human Decipherable Encryption Scheme - Encryption Schemes Based on Dice Codings - Conclusion and Future Work -- Non-Transferable Anonymous Credentials: Introduction, Scenario, and Related Work - Privacy and Data Security - Analysis of Non-Transferable Anonymous Credentials - Conclusion and Future Work -- Outlook and Appendix.
	Sommario/riassunto	Sebastian Pape discusses two different scenarios for authentication. On the one hand, users cannot trust their devices and nevertheless want to be able to do secure authentication. On the other hand, users may not want to be tracked while their service provider does not want them to share their credentials. Many users may not be able to determine whether their device is trustworthy, i.e. it might contain malware. One solution is to use visual cryptography for authentication. The author generalizes this concept to human decipherable encryption schemes and establishes a relationship to CAPTCHAS. He proposes a new security model and presents the first visual encryption scheme which

makes use of noise to complicate the adversary's task. To prevent service providers from keeping their users under surveillance, anonymous credentials may be used. However, sometimes it is desirable to prevent the users from sharing their credentials. The author compares existing approaches based on non-transferable anonymous credentials and proposes an approach which combines biometrics and smartcards. Contents Human Decipherable Encryption Schemes Visual Cryptography Non-Transferable Anonymous Credentials Authentication Target Groups Teachers, students and practitioners in the fields of cryptography and IT security About the Author Dr. Sebastian Pape is postdoctoral researcher at the Chair of Software Engineering at Technical University Dortmund.