**Grammar Study**

|  |  |  |
| --- | --- | --- |
| **Grammatical feature** | **Context** | **Translation** |
| **ARTICLES** | | |
| *“A/An”- numerical meaning of oneness* | 1. Frequently, users on the web need to show that they are, for example,  not **a robot**, old enough to access an age restricted video, or eligible to  download an ebook from their local public library without being tracked. [1:1]  2.  3. |  |
| *“Zero article” - with uncountable nouns* | 1.  2.  3. |  |
| *“A/An”- generic function* | 1. Scenario 2: **A cryptographer** walks into a bar. [1:27]  2.  3. |  |
| *“Zero article” - generic function* | 1. We now build a system for in-person age verification coupled with photographic verification. [1:27]  2.  3. |  |
| *“The”- generic function* | 1. Moreover, in **the event** the user has trustworthy secure hardware, they can self-issue the credential by attesting the hardware ran this notary check itself. [1:30]  2.  3. |  |
| *“A/An”- first mention + “The” - second mention* | 1.  2.  3. |  |
| *“A/An”- when modified by a descriptive attribute* | 1. Concretely, identity assertions using zk-creds take less than 150ms in **a real-world** scenario of using a passport to anonymously access age-restricted videos. [1:1]  2.  3. |  |
| *“The”- when modified by a limiting attribute* | 1. In contrast to scanning the user’s driver’s license, this reveals only the minimal information necessary. [1:27]  2.  3. |  |
| *“The” - unique objects and notions* | 1. For this scenario, **the only** issuer is our passport-based issuer, and the access criteria being proved are age, expiry, and non-cloning. [1:26]  2.  3. |  |
| *“The” by reason of locality* | 1.  2.  3. |  |
| *“The” when followed by an ordinal number* | 1. After **the first** time, the proof can be reused arbitrarily, until the user’s Merkle tree is updated by a new issuance. [1:29]  2.  3. |  |
| *“Zero article” when the noun is followed by a cardinal number* | 1.  2.  3. |  |
| **ACTIVE VOICE** | | |
| *Present Simple* | 1. We provide a toolchain to convert a passport into an anonymous credential. [1:26]  2.  3. |  |
| *Present Continuous* | 1.  2.  3. |  |
| *Present Perfect* | 1.  2.  3. |  |
| *Present Perfect Continuous* | 1.  2.  3. |  |
| *Past Simple* | 1.  2.  3. |  |
| *Past Continuous* | 1.  2.  3. |  |
| *Past Perfect* | 1.  2.  3. |  |
| *Future Simple* | 1.  2.  3. |  |
| *Future Perfect* | 1.  2.  3. |  |
| **PASSIVE VOICE** | | |
| *Passive Voice (Present Simple)* | 1.  2.  3. |  |
| *Passive Voice (Present Continuous)* | 1.  2.  3. |  |
| *Passive Voice (Present Perfect)* | 1.  2.  3. |  |
| *Passive Voice (Past Simple)* | 1.  2.  3. |  |
| *Passive Voice (Past Perfect)* | 1.  2.  3. |  |
| *Passive Voice (Future Simple)* | 1.  2.  3. |  |
| **VERBALS** | | |
| *Infinitive as a Subject or Attribute* | 1.  2.  3. |  |
| *Infinitive as a Predicate* | 1.  2.  3. |  |
| *Infinitive as an Adverbial Modifier* | 1.  2.  3. |  |
| *Complex Object with Infinitive* | 1.  2.  3. |  |
| *Complex Subject with Infinitive* | 1.  2.  3. |  |
| *Gerund as a Subject* | 1. Given issued credentials via passports, **building** a privacy-preserving age verification scheme with zk-creds is straightforward and requires no new cryptography: website developers need simply define the issuers they will accept and construct the access criteria they need using gadget. [1:26]  2.  3. |  |
| *Gerund as an Adverbial Modifier* | 1.  2.  3. |  |
| *Gerund as an Object (after preposition)* | 1. Finally, an issuer is able to revoke a credential if need be **by** simply **removing** it from the list.  2.  3. |  |
| *Gerund after Verbs (avoid, be worth, consider, finish, involve, allow, enable etc.)* | 1.  2.  3. |  |
| *Gerundial Complex* | 1.  2.  3. |  |
| *Participle as an Attribute* | 1.  2.  3. |  |
| *Participle as an Adverbial Modifier* | 1.  2.  3. |  |
| *Absolute Participial Construction* | 1.  2.  3. |  |
| *Complex Object with the Participle* | 1.  2.  3. |  |
| *Complex Subject with the Participle* | 1.  2.  3. |  |
| **MODAL VERBS** | | |
| *Can / could / be able to* | 1.  2.  3. |  |
| *May / might* | 1.  2.  3. |  |
| *Must / have to* | 1.  2.  3. |  |
| *Should / ought to* | 1.  2.  3. |  |
| **CONDITIONALS** | | |
| *Zero Conditional* | 1.  2.  3. |  |
| *I Conditional* | 1.  2.  3. |  |
| *II Conditional* | 1.  2.  3. |  |
| *III Conditional* | 1.  2.  3. |  |

**References:**

1. Michael Rosenberg et al. (2022). zk-creds: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure. *Cryptology ePrint Archive*. URL: <https://eprint.iacr.org/2022/878.pdf>.