TD 6 - Zero-knowledge protocol

The Guillou-Quisquater authentication protocol is the following one. A trusted third part (TTP), issuer of smart cards, has a public key (n, v). The integer n is the product of two large primes p and q; it is assumed that factorization of n is intractable. The integer $2 \leq v \leq n/2$ is chosen such that extracting v-root mod n is considered intractable.
For her public key, Alice uses the public information of her card, that corresponds to a string of characters (for instance, name of the issuer || card number || validity date || ...); this string is a sequence of bits that correspond to an integer $J \pmod n$.
The private key of Alice is an integer B such that $J.B^v = 1 \mod n$.
The authentication protocol involves the 3 folowing communications:

1. Alice chooses at random $r \in \{1, \ldots, n-1\}$, computes $T = r^v \mod n$ and sends T to Bob.
2. Bob chooses at random $d \in \{0, \ldots, v-1\}$ and sends d to Alice.
3. Alice computes $D = r.B^d \mod n$ and sends D to Bob.

To authenticate Alice, Bob computes $T' = D^v.J^d \mod n$. If $T' = T$ then Alice is authenticated; else she is rejected.

1. Prove that authentication is correct (soundness and completeness).

2. We assume that $r^v \mod n$ gives no knowledge on r. Argue that this authentication is a zero-knowledge protocol.

3. Previous protocol is extended as follows in order to provide Alice a protocol to sign any message M.

1. Alice computes $T = r^v \mod n$ with r chosen at random.
2. Alice computes $d = H(M||T)$ where H is a hash function on $\log_2 v$ bits resistant to collisions.
3. Alice computes $D = r.B^d \mod n$.
4. The signed message is $(M; \sigma)$ where $\sigma = (d||D||J)$ is the signature of M by Alice.

How Bob will verify the signature?